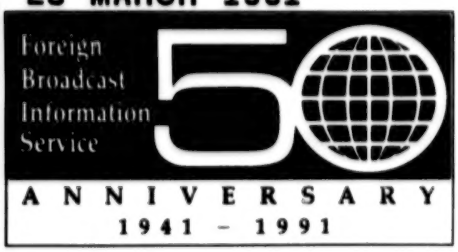
JPRS-JST-91-013
25 MARCH 1991



JPRS Report

Science & Technology

Japan

IEICE 1990 NATIONAL CONVENTION

JPRS-JST-91-013
25 MARCH 1991

SCIENCE & TECHNOLOGY
JAPAN

IEICE 1990 NATIONAL CONVENTION

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 various pages

[Selected papers from the Proceedings of the 1990 Spring National Convention of the IEICE held in Tokyo 18-21 Mar 90]

CONTENTS

Characteristics of Spread-Spectrum Land-Mobile Earth Stations for Mobile Satellite Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-245

[Article by T. Ikegami, N. Kadowaki, and S. Taira, Communications Research Laboratory, Ministry of Posts and Telecommunications; and N. Sato, S. Namiki, and Y. Seino, Toshiba Corporation]

[Text] **1. Introduction**

To gain a better understanding of the problems involved in using a spread-spectrum communications system for satellite communications with land-mobile stations, the authors used coherent matched filter technology[1] to develop a car-mounted spread-spectrum communications device. This report outlines the basic characteristics, including the bit error rate, of this device and describes the experiments we performed with this device using the ETS-V.

2. Circuit Specifications

Table 1 shows the circuit specifications when the ETS-V (at 150° E longitude) is used.[3] The required C/No. is assumed to be 44 dBHz with a chip rate of 2.4552 MHz, a bit rate of 2.4 kbps, and a permissible bit error rate (BER) of 10^{-4}. Since the purpose of this paper is to provide an understanding of the basic characteristics, values are calculated assuming that there is no other station involved in communications simultaneously. The forward link from the base earth station to the mobile station has a small margin because3 it is dominated by the downlink circuit from the satellite. In contrast, the return link from the mobile station to the base earth station has a larger margin, although it is dominated by the uplink circuit. Thus, the transmitting power of the mobile station can be no more than 10 W.

3. Basic Characteristics

Figure 1 shows the BER with respect to the C/No. Since the transmitting and receiving frequencies are not the same, the data was obtained using a frequency shifter with RF foldback. The solid line in the figure is the theoretical curve with coherent detection PSK (differential encoding).

Table 1. Circuit Specifications

Base Earth Station → Mobile Earth Station

Base station EIRP/CH	60.2 dBW
Uplink circuit propagation loss (6 GHz)	199.4 dB
Satellite G/T Uplink circuit C/No. Transponder gain Satellite EIRP/CH	-8.1 dBK 81.1 dBHz 127.7 dB 26.7 dBW
Downlink circuit propagation loss (1.5 GHz)	187.6 dB
Receiving antenna gain Circuit loss Receiving power Mobile station G/T Downlink circuit C/No.	6.0 dBi 0.7 dB -156.3 dBW -19.0 dBK 48.0 dBHz
Overall C/No.	48.0 dBHz
Required C/No. Circuit margin	44.0 dBHz 4.0 dB

Mobile Earth Station → Base Earth Station

Mobile station transmitter output Antenna gain Circuit loss Mobile station EIRP	13.0 dBW 6.0 dBi 0.7 dB 18.3 dBW
Uplink circuit propagation loss (1.6 GHz)	188.2 dB
Satellite G/T Uplink circuit C/No. Transponder gain Satellite EIRP/CH	-4.5 dB 54.1 dBHz 127.8 dB -3.9 dBW
Downlink circuit propagation loss (5 GHz)	198.2 dB
Base station G/T Downlink circuit C/No.	32.7 dBK 58.9 dBHz
Overall C/No.	52.9 dBHz
Required C/No. Circuit margin	44.0 dBHz 8.9 dB

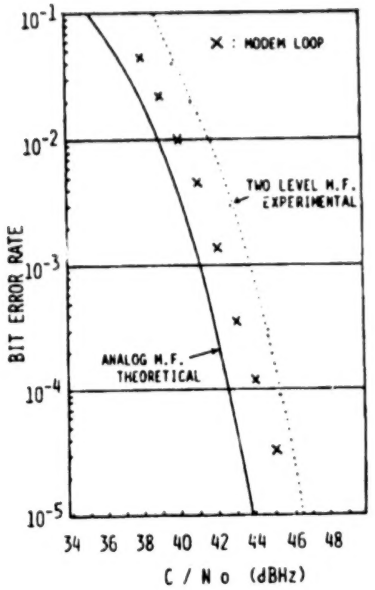


Figure 1. Bit Error Characteristics

The degradation from the theoretical values is about 1.2 dB. Because the correlator used with the coherent matched filter (CMF) was an 8-bit quantification type, degradation due to quantification can be ignored. For reference, the results of experiments obtained with the device using a two-level quantification correlator[3] are shown by the dotted curve. A comparison of these curves shows the characteristic improvement of multilevel quantification.

The quality of speech obtained when using a 2.4 kbps LPC is good and is unaffected by errors provided that the BER is around 10^{-4}.

Among the sync characteristics, the initial acquisition time is within 1 second when a 10 kHz AFC is included, regardless of the circuit C/No. Almost the whole of this period is used for frequency search, and loop system phase synchronization is completed within a few tens of milliseconds.

4. Conclusion

The basic characteristics, including the BER, of the spread-spectrum mobile station we developed have been described above. The details of the satellite communications experiments we performed after mounting the station in a car will be reported in the lecture meeting. The evaluation of the multiple-access characteristics and interference characteristics with respect to the SCPC communication waves are left for future investigation.

References

1. Hamamoto, et al., "Spread-Spectrum Communications Equipment for Satellite Communications Featuring Direct Data Demodulation Using Matched Filters," TRANSACTIONS OF IEICE, J-698 No 11, Nov 86, pp 1540-1547.

2. Sato, et al., "Spread-Spectrum Communications Equipment for Mobile Satellite Communications: Outline of Device," Draft written for 1990 IEICE National Convention.

3. Suzuki, et al., "Mobile Satellite Communications Systems Using Engineering Test Satellite V (ETS-V)," RADIO RESEARCH INSTITUTE QUARTERLY, Vol 34, Mar 88.

Spread-Spectrum Communications Equipment for Mobile Satellite Communications: Hardware Implementation

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-246

[Article by N. Sato, S. Namiki, and Y. Seino, Toshiba Corporation; and N. Hamamoto, R. Suzuki, and T. Ikegami, Communications Research Laboratory, Ministry of Posts and Telecommunications]

[Text] **1. Introduction**

A spread-spectrum (SS) communications system is believed to be suitable for use in mobile satellite communications because it creates little interference with other communications systems and because it provides easy random access. However, to implement such a system, it will first be necessary to increase the speed of the AFC, which compensates for Doppler shift and frequency drift, and to reduce the pull-in period. This report describes our newly developed SS communications equipment for mobile satellite communications in which these problems have been solved by using multilevel digital matched filters.

2. Outline of Hardware

The configuration of the equipment is shown in Figure 1, and the principal specifications are shown in Table 1.

2.1 Antennas

The receiving and transmitting antennas are independent. They are higher mode microstrip antennas. They are omnidirectional in azimuth and have fixed directivity in elevation, being pointed toward the satellite. The elevation angle of the beam center is 55° so that the ETS-V satellite can be located without a tracking mechanism when the equipment is used within Japan.

2.2 HPA

HPA output power is 20 W. The SS modulation uses the BPSK system, and class A operation is used to prevent broadening of the spectrum.

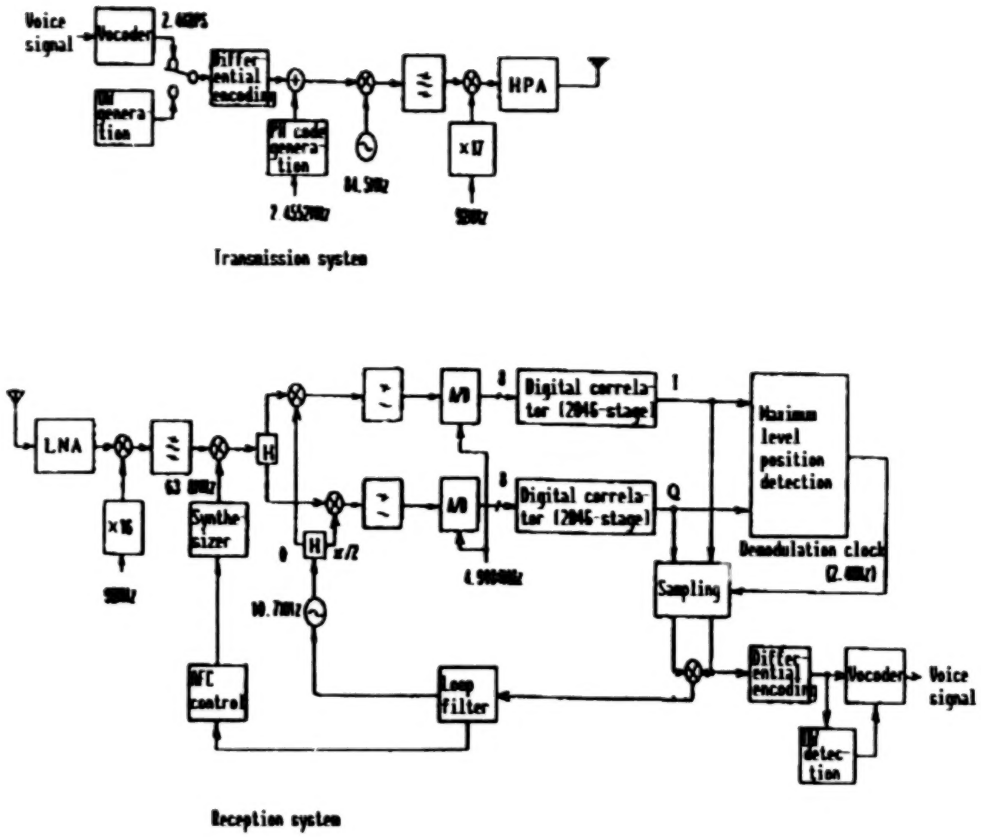


Figure 1. Configuration of Spread-Spectrum Communications Equipment for Mobile Satellite Communications

Table 1. Specifications for Spread-Spectrum Communications Equipment for Mobile Satellite Communications

1. Antenna gain	6 dBi
2. TX/RX center frequencies	1648.5 MHz (TX)/1546.5 MHz (RX)
3. HPA	Class A, 20 W
4. Voice coder/decoder	LPC vocoder
5. Information transmission rate	2.4 kbps
6. Spreading code	PN code, code length 1023
7. Chip rate	2.4552 MHz
8. Spread modulation system	BPSK
9. Spread demodulation system	CMF-SS method, coherent detection
10. Matched filters	2046-stage multilevel digital matched filters
11. AFC range	±10 kHz
12. Sync establishment time	1 second

2.3 Modem

The data rate of the modulator/demodulator circuits is 2.4 kbps, and speech is coded using an LPC system vocoder. The data to be transmitted is differentially encoded, then the coded PN is added at MOD2, and the carrier is modulated by BPSK. The PN chip rate is 2.4552 MHz, the PN code length is 1023, and the cycle corresponds to one clock of the data rate. Unique words (UWs, 31-bit PN patterns) are transmitted continuously at the start of transmission.

The received signal is first detected by quadrature detection, then A/D converted (8-bit conversion) at twice the PN clock frequency, and is input to the matched digital filters. As a correlation peak appears at every 2,046 clocks in each matched digital filter output, a clock is regenerated to sample the correlation peaks by peak position detection. Then, using the carrier phase error information contained in the I and Q correlation peaks, a carrier regeneration loop is formed to perform coherent detection (CMF-SS method). Previous designs used bilevel matched filters, but the new equipment uses multilevel matched filters both to reduce phase jitter in the regenerated carrier and to prevent demodulation loss due to the use of bilevel filters. The demodulated data is differentially decoded. When a UW is detected, the subsequent data is input to the LPC vocoder.

The operation of the AFC is different both before and after the detection of UW. Before UW detection, it sweeps the local frequency, fixes the frequency so as to maximize the correlation peaks, and waits for the carrier regeneration loop to be locked. After UW detection, it tracks the frequency using the carrier regeneration loop and, if the frequency goes beyond the tracking range, varies the local frequency (in 10-Hz steps) to deal with it. Figure 2 [not reproduced] is a photograph of the device.

3. Conclusion

We developed a new device for SS communications by incorporating multilevel digital matched filters to increase AFC speed, reduce the pull-in period, and decrease demodulation loss. This device was developed with the cooperation of the Communications Research Laboratory and Toshiba Corporation. The next step will be to conduct experiments using the ETS-V satellite.

Performance of Constant-Envelope Spread-Spectrum BPSK Modem

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-247

[Article by A. Yamashita, N. Iizuka, and K. Matsuyama, Fujitsu Laboratories, Ltd., Kawasaki; and E. Morikawa and T. Ikegami, Communications Research Laboratory, Ministry of Posts and Telecommunications]

[Text] **1. Introduction**

Mobile communications/positioning systems are attracting attention because of their capability to position a mobile station while simultaneously communicating with it.[1]

Most mobile communications/positioning systems use the spread-spectrum (SS) communications system to improve distance measuring accuracy and to prevent signal interference. In addition, in order to reduce the power required by the mobile station, it is desirable to use the constant-envelope modulation system, which features highly efficient class C amplifiers, as the HPA.

To collect basic data for the development of a communications/positioning system, the authors made a prototype direct-spread (DS) SS modem that uses the constant-envelope BPSK modulation method and measured its characteristics by the IF back-to-back method. This report describes its bit error rate (BER) characteristics.

2. Constant-Envelope Technology

The experimental constant-envelope BPSK (CE-BPSK) modulator features complementary signal insertion by baseband processing.[2] Its operating principle is shown in Figure 1. This method is suitable for digitization. It can be configured simply and stably, and its size can be reduced by the use of large-scale integration. Although transmission power efficiency may be degraded by an amount corresponding to the complementary signal, the degradation that occurs when a 100 percent roll-off filter is used as the transmitted waveform shaping filter is about 1.7 dB, which is smaller than the overall efficiency improvement made possible by the use of a class C HPA.

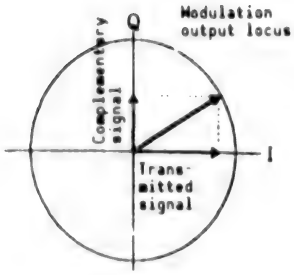


Figure 1. Constant Envelope Provided by Complementary Signal Insertion

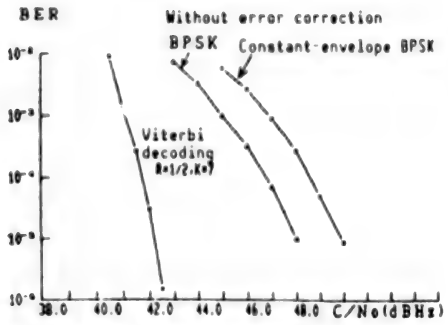


Figure 2. Actual Measured BER Values

For this system, degradation due to interference with the complementary signal occurs when there is a correlation between the complementary signal used with the experimental modulator was selected to minimize correlation with the PN signal.

3. Experimental Results

Table 1 shows the specifications of the experimental modem, and Figure 2 shows the BER as measured by the IF back-to-back method. Although the transmission power is degraded by 1.7 dB due to the insertion of a complementary signal for providing a constant envelope, the degradation caused by BER is about 1.8 dB, so there is actually no overall degradation due to interference of the complementary signal.

The encoding gain of the Viterbi decoder is about 7.8 dB (BER: 10^{-5}), which agrees closely with the theoretical value. Therefore, it was also confirmed that there is nothing degrading the correction capability.

Table 1. Specifications of Experimental Equipment

IF frequency	70 MHz
Information rate	2.4 kbps (FEC ON)/4.8 kbps (FEC OFF)
Modem bit rate	5 kbps
Chip rate after spreading	1.275 Mbps
Error correction	R=1/2, K=7 soft judgment, Viterbi decoding

4. Conclusion

The authors of this report devised a constant-envelope BPSK, DS-SS modem for use in a communications/positioning system, measured its bit error rate, and confirmed that there is no degradation of the bit error rate or error

correction capability due to the interference of the complementary signal or other factors.

The results of this experiment demonstrate that the constant-envelope BPSK modulation with baseband-processing complementary signal insertion is a constant-envelope modulation method particularly suitable for spread-spectrum communications and effective for use in communications/positioning systems.

References

1. Morikawa, et al., "Proposal and Experiment Project for Combined Communications/Positioning System Using Two Geostationary Satellites," IEICE NEWS, SANE88-21.

2. Yazdani, H., et al., "Constant-Envelope Band-Limited BPSK Signal," IEEE COM-28, pp 889-897.

3. Ushiyama, et al., "High-Accuracy Delay Sync Circuit With Baseband Processing," to be presented at the Spring 1990 IEICE National Convention.

Fast SS-FH Differential Despreading Method for Consumer Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-391

[Article by A. Kajiwara and M. Nakagawa, Faculty of Science and Technology, Keio University]

[Text] **1. Introduction**

This report proposes a new differential despreading method for applying frequency modulation to an FH signal. This method performs frequency heterodyne processing at the same time as differential despreading to obtain a narrow-band IF frequency. If different IF frequencies already have been assigned to nearby stations, only the signal from the desired station passes through the narrow-band BPF and is demodulated. In addition, the narrow-band signal and other output from the RF amplifier are separated into low-frequency components and harmonic components, but these components will not be demodulated because they are substantially different from the IF frequency and thus are passed by the BPF.

2. SS-FH Differential Despreading System

Figure 1 shows a block diagram of the proposed differential despreading system.

2.1 Fast SS-FH Signal

When fast FH is performed with N chips per information bit, the transmitted signal, s(t), is expressed as follows:

$$s(t) = [s_1, s_2, \cdots, s_{N/2}, \cdots, s_N]$$

The signal of each chip, s_k (k=1, $\cdots$, N) is expressed as follows:

$$s_k = \begin{cases} \cos(\omega_k t + \theta(t)) & (1 \leq k \leq N/2) \\ \cos(\omega_k - \omega_{IF})t) & (N/2 + 1 \leq k \leq N) \end{cases}$$

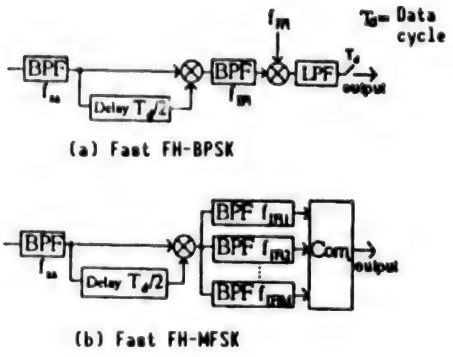


Figure 1. Block Diagrams of Differential Despreading System

Here, $\theta(t)$ is the information signal $\theta t = (0, \pi)$. The modulation is FH-BPSK when $\theta(t) = M \cdot \Delta\omega$ and FH-MFSK when $\theta = MN\_\omega$. ω_{IF} is one of the IFs previously assigned to the stations.

2.2 System Characteristics

Figure 2 shows the error rate characteristic when narrow-band interference, J, is present. Here, it is assumed that the number of hops per bit, N, is 10 and that the narrow-band interference is CW interference. Figure 2 demonstrates that the conventional system becomes totally incapable of reception if the SJ ratio drops to 0 dB or less, and also that the proposed system can provide sufficient safeguards against narrow-band interference. This is because the proposed system can eliminate the self-correlation component of the interference wave due to differential despreading and can suppress the cross-correlation component between the signal and interference wave, etc., by spectrum spreading the FH signal. Figure 3 shows the error rate characteristic when the number of hops, N, is varied. Here, the SJ ratio is assumed to be -10 dB. Figure 3 demonstrates that increasing the number of hops, N, can improve the characteristic dramatically. This is because the influence of the interference wave is spread as the number of hops, N, per information bit increases. Figure 4 shows the characteristic when an interfering station is present. Here, it is assumed that the number of hops, N, is 10, the SNR is 20 dB, and that the receiving power from the interfering station is 0 dB, which is equal to that from the desired station. Figure 4 demonstrates that the quality is degraded drastically if the number of interfering stations, K, increases. This is due to the increase of collisions between the hopping frequencies of different stations. The figure also demonstrates that the increase in the number of hopping frequencies used, L, decreases the probability of hopping frequency collisions, thereby reducing the influence of interference from other stations. Assuming that the BER with which data demodulation is possible is 0.002 or less, and when N = 10 and L = 10, the number of simultaneous accesses is 5, and the frequency efficiency, n, is 50 percent.

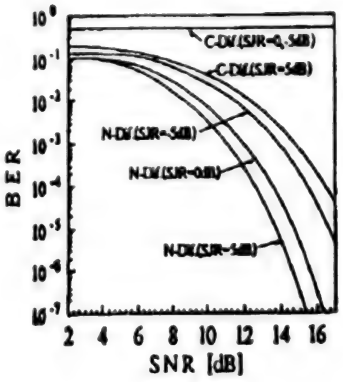


Figure 2. Error Rate for Narrow-band Interference

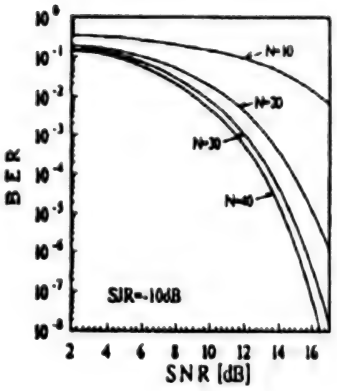


Figure 3. Error Rate Vs. Number of Hops (For different numbers of hops)

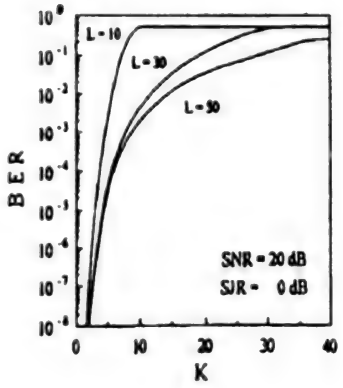


Figure 4. Error Rate Vs. Number of Interfering Stations

3. Conclusion

This report proposes a new differential despreading method that is resistant to narrow-band interference and interstation interference from other stations, and demonstrates its effectiveness. It has been confirmed that this method can greatly improve interference resistance and random access capability (multiple stations). Consequently, we believe this method is effective not only for mobile communications but also for consumer communications where simplicity and compact size are required.

References

1. Kajiwara and Nakagawa, "Fast SS-FH Differential Despreading Method for Consumer Communications," IEICE NEWS, RCS, 18 Jan 90.

Frequency-Hopping Spread-Spectrum Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-266

[Article by N. Kimura, H. Fujii, T. Miyashita, and C. Sato, Faculty of Science and Technology, Keio University]

[Text] **1. Introduction**

The authors constructed a transceiving communications apparatus in a laboratory environment by introducing the FH-SS method to a data communications system using power lines with poor circuit quality. In examining the equipment, special attention was paid to the sync acquisition algorithm.

2. Transmitter/Receiver Configuration

The transmitter consists of a single-chip CPU (HD6303X) that incorporates code sequence generator and code modulator functions. The receiver is a CPU 80386, which has more functions than the CPU used with the transmitter (Figure 1). The received signal is sampled at 10 kHz and converted into an 8-bit digital signal.

The main parameters of this system are as shown below.

Spreading sequence:	Reed-Solomon sequence with sequence length of 31
Hopping rate:	20 hps
Frequency band:	500 Hz~5 kHz
Data modulation method:	FSK (f_0 ±15 Hz)

3. Receiver Operating Principle

Spectrum spreading by the frequency hopping method is performed by switching the signal carrier frequencies randomly and discretely within the given band and sweeping them. In our research, we performed an experiment by switching the carrier frequencies from f_1 to f_{31} for every chip length of T_H (Figure 2(a)).

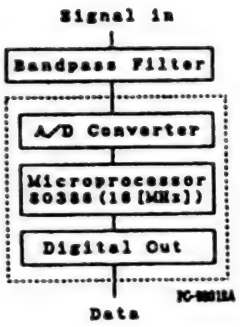


Figure 1. Block Diagram of FH-SS Receiver

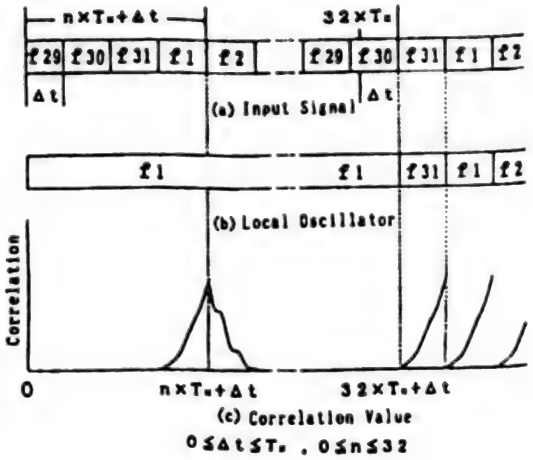


Figure 2. Acquisition Process

The receiver should first acquire sync with respect to the discretely switched carrier frequencies. To achieve this, the receiver generates frequency f_1 continuously and correlates it with the input signal. As the correlation value reaches its peak when the input signal coincides with f_1, sync can be acquired with reference to that time (Figures 2(b) and (c)). This method allows sync to be acquired by calculating the correlation value peak time during a period of 33 x T_H. As a result, sync in this system can be acquired in 1.625 seconds on average, which is 6.125 seconds shorter than previous systems.[1] In addition, sync can be acquired even when the input signal level is unknown because acquisition does not use a threshold. Also, acquisition is perfect because the correlation value reaches its peak at the instant the carrier frequency is switched. Therefore, sync does not require tracking provided that clock accuracy satisfies the required communications time.

Once sync is required, the frequencies generated by the receiver are switched every T_H, the correlation value is calculated for each frequency, and demodulation of the data is started.

A threshold is determined from the maximum value of the correlation values measured during sync acquisition, and sync acquisition is restarted if the correlation value drops below the threshold for a period of 5 x T_H.

4. Characteristics in Laboratory Environment

Figure 3 shows SNR versus BER values with respect to white noise. When a bit is transmitted on one channel, a bit error rate of 10^{-3} is achieved at an SNR of around -30 dB. When a bit is transmitted on three channels, the same bit error rate can be achieved at an SNR of around -32 dB. A triangular interference of 50 dB was used as a control. No influence is observed even at an SNR of -36 dB.

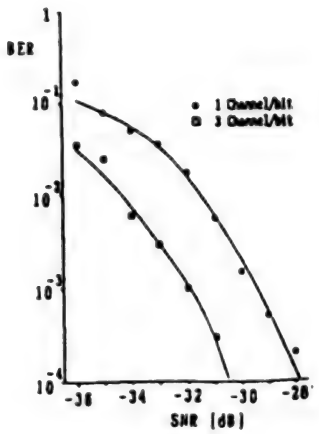


Figure 3. Bit Error Performance of FH-SS Receiver

5. Conclusion

This paper proposes a new method for FH sync acquisition and describes experiments that have been performed with it. This method can provide a faster and more accurate sync acquisition compared to the conventional sliding correlation system, and can be used for communications up to around -30 dB in a white noise environment. The reliability of the system can be improved further by performing all correlation value calculations by means of software. Although some improvements may be necessary for multiplexed communications in the future, we still believe that this principle of sync acquisition is sufficiently effective.

In closing, the authors would like to express their gratitude to Professor Hideo Nojima for the kindness he always showed them.

References

1. Wada, Kimura, Miyashita, and Sato, "Power Line Communications Using Frequency Hopping," Proceedings of the Spring 1990 IEICE National Convention, B-445, 1988.

Ultrasmall Data Carrier Using Spread-Spectrum Technique for Consumer Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-269

[Article by K. Harada, A. Kajiwara, and M. Nakagawa, Faculty of Science and Technology, Keio University; and K. Takeuchi, Tokyo Keiki Company]

[Text] **1. Introduction**

In the field of factory automation, security, and physical distribution control, data carrier technology is showing remarkable progress. With this technology, a data carrier consisting of a storage device, such as a semiconductor memory chip, to which a short-distance communications function is added, can be attached to a moving "object" and information is read from or written into the storage device without contact with that "object."

However, when an ultrasmall magnetic-coupling data carrier is used in a poor radio environment, such as in a factory or workshop, it is subject to the strong influence of noise and interference, and the reliability of the communications is degraded. Also, the use of magnetic coupling in the communication medium results in a significant attenuation of transmission signal power, and thus data can be transferred only for a short distance.

This report deals with the results obtained from experiments performed by applying memory storage and batch processing to an ultrasmall data carrier demodulation system using the spread-spectrum (SS) technique.

2. Experimental Systems and Methods

Figure 1 is a block diagram of the ultrasmall data carrier communications system used in the experiments. Here, a 1 MHz spread signal generated using Manchester Gold codes M_0 and M_1 with code lengths of 31 is transmitted and received via a coil. The receiver performs digital signal processing using an 8-bit, 20-MHz A/D converter.

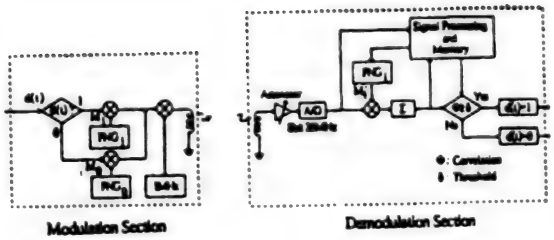


Figure 1. Block Diagram of Data Carrier

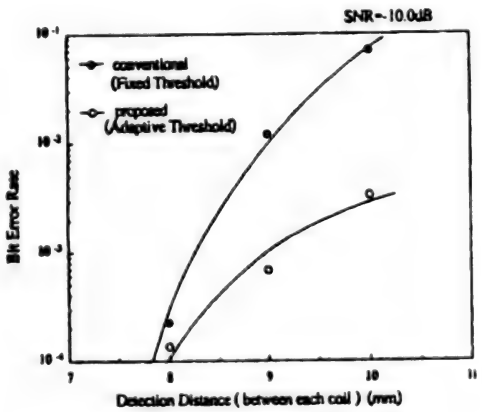


Figure 2. Detection Distance Vs. Bit Error Rate

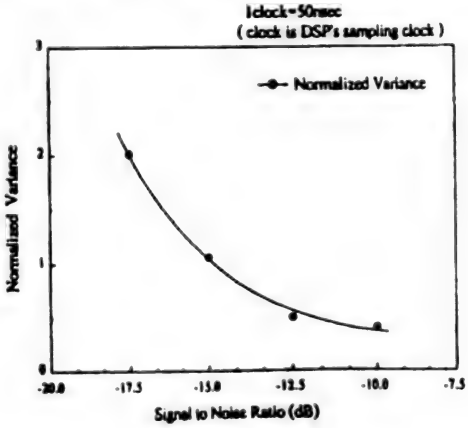


Figure 3. SNR Vs. Normalized Variation Characteristic

3. Results of Experiments

Experiment (1)

The adaptive threshold technique was applied to set the threshold at the optimum value according to the transfer distance. The threshold is set by storing the correlation values (data amount) obtained in sync detection operations in a 100-point memory and reading the stored data simultaneously. Figure 2 shows that the adaptive threshold technique can improve performance considerably compared to the conventional method, which uses a fixed threshold.

Experiment (2)

When tens or hundreds of data points are transmitted continuously and the data received are stored in batches in a memory, it is important to acquire sync from the first data point because this facilitates sync acquisition and subsequent data points. Therefore, M_1 is transmitted with the first data point assigned as a preamble, and the experiment was designed to identify the sync timing variation with respect to noise. As shown in Figure 3, it was determined that the sync timing variation is within ±2 clock (±100 nanoseconds) at $-17.5\ dB \leq SNR \leq -10\ dB$.

4. Conclusion

The authors conducted experiments based on the idea of introducing memory storage and batch processing in the demodulator of an ultrasmall data carrier using the spread-spectrum technique to improve performance. The results showed that this method is fairly promising.

Acknowledgements

The authors would like to thank Tokyo Keiki Company and the members of the Nakagawa Research Office for their instructive discussions and advice.

References

1. Harada, Kajiwara, Takeuchi, and Nakagawa, "Characteristics of Ultrasmall Data Carriers Using Spread-Spectrum Communications Technique," IEICE NEWS, SSTA89-43, Nov 89.

Code Noise of DS-SS Communications Using General Chip Waveforms

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-272

[Article by T. Miura and K. Miyauchi, Faculty of Engineering, Science University of Tokyo]

[Text] **1. Introduction**

Analyses of DS-SS communications systems are usually based on spectrum techniques, and there are few examples of use of waveform techniques.[1] However, waveform analysis is advantageous in some cases, for example, with regard to SNR degradation due to sync fluctuation. This report describes an attempt to obtain the SNR of the code noise with respect to the average power[1] as a first step toward an analysis of a DS-SS communications system using general chip waveforms with different reference signals on the transmitter and receiver sides. This experiment demonstrated that the average power of code noise near the sync point can be reduced by providing an optimum chip waveform at the receiver side according to a given chip waveform from the transmitter side.

2. Analytical Model

Figure 1 shows the system model and Figure 2 shows concept diagrams of chip waveforms. With this model, the demodulated output $\hat{m}(T_M)$ from the integrator can be expressed by the following formula:

$$\hat{m}(T_M) = \frac{1}{T_M}\int_{t_1/2}^{T_M-t_1/2} m(t)\,b_1(t)\,b_2(t+\tau)\,dt$$

$$= \pm R_M(\tau) \qquad (1)$$

Here, $R_M(\tau)$ is referred to as the partial self-correlation function. Because the amplitude of its signal component is an average value and the average power of its noise component is spread, the SNR can be expressed as follows:

$$SNR = \frac{P_s}{P_{nc}} = \frac{\{E[R_M(\tau)]\}^2}{V[R_M(\tau)]} \qquad (2)$$

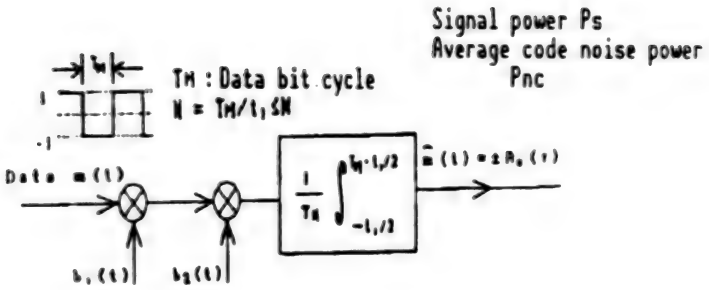


Figure 1. System Model

Note: $b_1(t) = \sum_{n=-\infty}^{\infty} a_n g_1(t-nt_1)$, $b_2(t) = \sum_{m=-\infty}^{\infty} a_m g_2(t-mt_1)$

M sequence: (an), an = ±1, code length N, cycle T, $t_1 = T/N$

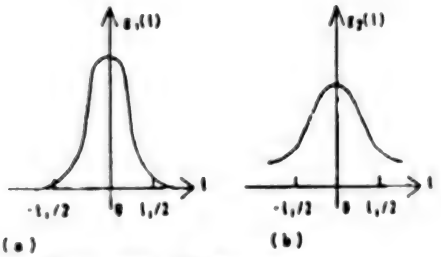


Figure 2. Chip Waveform Concept Diagram

Note: It is assumed that $t_1 \ll T_M$, and that waveform spreading is smaller than T_M.

3. Signal Power and Average Code Noise Power

(i) $R_M(\tau)$ is as follows:

$$R_M(\tau) = \frac{1}{T_M}\int_{-t_1/2}^{T_M-t_1/2} \sum_{n=-\infty}^{\infty} a_n g_1(t-nt_1) \cdot \sum_{m=-\infty}^{\infty} a_m g_2(t-mt_1+\tau)\,dt \tag{3}$$

When the chip waveform sequence of $b_1(t)$, whose center is located outside the integration section $(-t_1/2,\ T_M-t_1/2)$, is ignored and it is assumed that the waveform spreading of $g_1(t)$ and $g_2(t)$ is smaller than T_M, formula (3) can be approximated as follows:

$$R_M(\tau) = R_{g_1g_2}(\tau) + \frac{1}{M}\sum_{k=-(N-1),\,k\neq 0}^{N-1} C_M(k)\,R_{g_1g_2}(\tau-kt_1) \tag{4}$$

Here, when $R_{g_1g_2}(\beta)$ is assumed to be the correlation function of chip functions $g_1(t)$ and $g_2(t)$ and $C_M(k)$ is assumed to be the correlation function of the code, they can be defined by the following formulas:

$$R_{g_1g_2}(\beta) = \frac{1}{t_1}\int_{-\infty}^{\infty} g_1(t)\, g_2(t+\beta)\, dt \tag{5}$$

$$C_M(k) = \sum_{n=0}^{M-1} a_n a_{n+k} \tag{6}$$

(ii) Since it is already known that the average value of $C_M(k)$ is -M/N, signal power P_s can be expressed as follows:

$$\begin{aligned} P_s &= \{E[R_M(\tau)]\}^2 \\ &= \{R_{g_1g_2}(\tau) - \frac{1}{N}\sum_{k=0} R_{g_1g_2}(\tau - kt_1)\}^2 \end{aligned} \tag{7}$$

(iii) As for the average power of code noise, P_{nc}, the mean square value of $R_n(\tau)$ is calculated first:

$$\begin{aligned} &E[R_M^2(\tau)] \\ &= R_{g_1g_2}^2(\tau) - \frac{2}{N} R_{g_1g_2}(\tau) \sum_{k=0} R_{g_1g_2}(\tau - kt_1) \\ &+ \frac{1}{M^2} \sum_{k=0} \sum_{k'=0} E[C_M(k)\, C_M(k')] \\ &\cdot R_{g_1g_2}(\tau - kt_1)\, R_{g_1g_2}(\tau - k't_1) \end{aligned} \tag{8}$$

Meanwhile, E $[C_M(k)\ C_M(k')]$ can be expressed using the constant η_M (k, k') given to each M sequence[2] as follows:

$$E[C_M(k)\, C_M(k')] = \eta_M(k, k')\,(1 + \frac{1}{N}) - \frac{M^2}{N} \tag{9}$$

Therefore, the spreading or $R_M(\tau)$ is as follows:

$$\begin{aligned} P_{nc} &= V[R_M(\tau)] \\ &= \sum_{k=0} \sum_{k'=0} \{(1+\frac{1}{N})(\frac{\eta_M(k, k')}{M^2} - \frac{1}{N})\} \\ &\cdot R_{g_1g_2}(\tau - kt_1)\, R_{g_1g_2}(\tau - k't_1) \end{aligned} \tag{10}$$

(iv) The SNR of the code noise with respect to the average power can be obtained from formulas (2), (7), and (10). Formula (10) shows that reducing the waveform spreading of $R_{g_1g_2}(\beta)$ decreases the average power of code noise near the sync point. Therefore, to prevent waveform spreading of $R_{g_1g_2}(\beta)$ when the received waveform is spread due to bandwidth limiting, the reference signal on the receiver side should use impulses as the chip waveform.

4. Concrete Example

Figure 3 shows a concrete example. The rectangular pulse-impulse makes it possible to obtain $P_{nc} = 0$ in the wide area of $(-t_1/2,\ t_1/2)$.

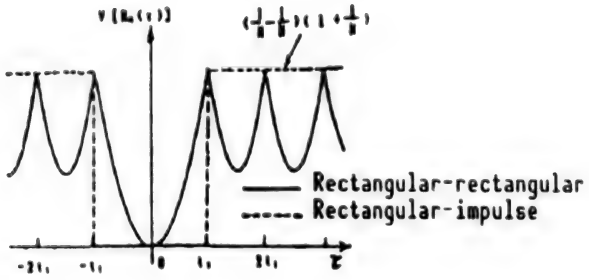


Figure 3. Average Power of Code Noise

5. Conclusion

In the above, the code noise SNR with respect to average power when the reference signals in the transmitter and receiver have different chip waveforms was obtained. As a result, it was demonstrated that the use of different chip waveforms can reduce the average power of code noise near the sync point. However, as it is thought that external noise may be increased, the authors are planning to undertake a more comprehensive examination that takes into account external noise, interference noise, and jitter. As for the variable $\eta_n(k,k')$, a separate report will be prepared.

Acknowledgements

The authors would like to express their deep gratitude to Lecturer Tsutomu Inasaka of the Science University of Tokyo for his wide range of assistance.

References

1. Cooper, G.R. and McGillem, C.D., "Modern Communications and Spread Spectrum," McGraw-Hill, 1986.

2. To be reported separately.

Spread-Spectrum Decoder Utilizing Neural Network

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-274

[Article by T. Kajiwara and K. Kitayama, NTT Transmission Systems Laboratories]

[Text] **1. Introduction**

The spread-spectrum (SS) communications system has a number of excellent features, including privacy, the fact that network synchronization and concurrence control are not necessary, and small transmission delay at busy times. These features can be exploited by an optical SS system[1] that takes advantage of the wide-band characteristics of optical fibers. This report proposes the use of a neural network (NN) for decoding of SS signals. It has been demonstrated by simulations that the decoding capability can be improved thereby. The authors have already proposed an SS decoding method using the Hopfield model and the Perceptron model,[2] and have obtained favorable results from simulations. For this study, the authors performed adaptive learning using a three-layer Perceptron and obtained a favorable error recovery result, which is described in this report.

2. Decoding Technique Utilizing NN

It should be noted that the SS technique can be used for spreading on the time axis.[1] Figure 1 shows the configuration of a three-layer Perceptron model NN.[3] Several spread code patterns are stored in this circuit based on learning. The received signal, which has been coded (spread) at the transmitter side and is affected by noise and jamming, is serial-to-parallel converted and applied to the input layer shown in the figure. The result of received pattern judgment is output depending on which of the output layer elements is lit. The number of input layer elements coincides with the spread code length. The number of output layer elements to be prepared is the same as the number of patterns. After having completed the learning for storage, unnecessary outputs can be removed. For example, when the weighting is to be transferred to another circuit after the completion of learning, privacy between users can be maintained perfectly by transferring only the part related to a single output and limiting the number of outputs to one.

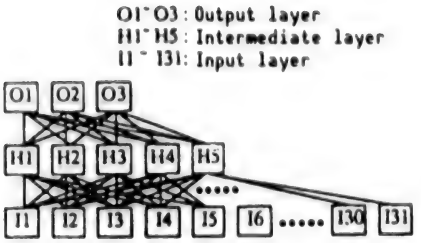


Figure 1. Configuration of Spread Code Decoding Circuit (Three-layer Perceptron)

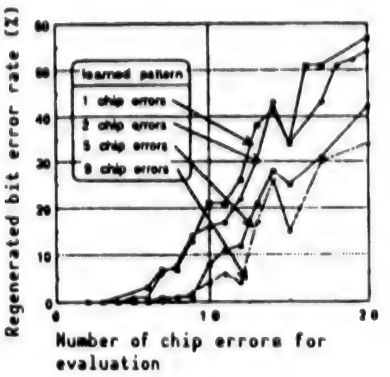


Figure 2. Error Recovery Characteristics

3. Simulation

Three-spread code patterns, each having a code length of 31, are stored as shown by patterns A, B, and C below.

Pattern A = '11111001 10100100 00101011 1011000'
Pattern B = '00100110 00010110 10100011 1011111'
Pattern C = '11110110 01110000 11010100 1000101'.

These patterns are linear M sequences,[4] and the cross-humming distances are between 16 and 20.

The learning rule is based on back propagation, the temperature is 1 and the learning rate is 0.5. The learning pattern error recovery performance is evaluated by first converging the patterns with error-free patterns A, B, and C, and then letting the circuit learn four kinds of 100 patterns, each containing 1, 2, 5, or 9 random error chips. The 100 patterns containing error chips used for evaluation are different from those used in learning and are generated in a random manner.

4. Results and Discussion

Figure 2 shows the error recovery performance is improved as patterns with larger numbers of chip errors are learned. In general, error recovery is not governed directly by the number of error chips learned. However, the result is not really satisfactory if the pattern learned contains nine errors or more. Assuming that the number of error chips is m, the number of patterns containing m chip errors is ${}_{31}C_m$. For example, when m = 15, the total number of patterns is 3×10^9, which is 3 million times the 100 patterns which were used in learning. However, as shown in Figure 2, the generalization of the NN provides the ability to judge many patterns that are not presented here. The error recovery performance is expected to be improved further by increasing the number of patterns learned to more than 100.

5. Conclusion

The authors have proposed an SS decoder utilizing the generalization characteristic of the NN, which makes it possible to deal with more chip error patterns based on learning some of them (as a proverb says, to know ten by hearing one), and have confirmed its effectiveness. The error patterns of the transmission channels can vary depending largely on the environment of the receiver. The proposed method is suitable for use in the SS decoder because the error characteristic can be improved by having the receiver learn to adapt to the error patterns inherent in its environment. Possible subjects for future examination include the selection of learning patterns and their number, identifying the amount of learning required (because overlearning narrows the generalization effect), the learning method itself (how to provide initial values), and the method for increasing the code patterns (whether sequences other than the orthogonal M sequence can be used or not).

References

1. Kajiwara and Kitayama, Proceedings of the Fall 1988 IEICE National Convention, B-407.

2. Kajiwara, Ito, and Kitayama, Proceedings of the Spring 1988 IEICE National Convention, B-743.

3. Rumelhard, D.E., et al., PARALLEL DISTRIBUTION PROCESSING, Vol 1.

4. Dixon, R.C., "Spread-Spectrum Technique," Jatec Shuppan (publisher).

Study of Code Sequence for Frequency Hopping Spread-Spectrum Communications System Using Optical Orthogonal Codes

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-280

[Article by S. Sasaki and G. Marubayashi, Nagaoka University of Technology]

[Text] **1. Introduction**

In terms of code sequences for use with the spread-spectrum (SS) communications system, many sequences have been proposed for direct-spread (DS) systems, but very few have been proposed for frequency-hopping (FH) systems. This report proposes a method for forming a code sequence for FH systems by extending the concept of the optical orthogonal code (OOC),[1] and examines its correlation characteristics.

2. Code Sequence Forming Method

The OOCs that will be the basis of the target sequence are assumed to be A and B. Their lengths are M and N, and their weights, w_A and w_B, respectively. In this case, A and B can be represented by the following vectors:

$$A = (a_1, a_2, a_3, \cdots, a_{M-1}) \tag{1}$$

$$B = (b_1, b_2, b_3, \cdots, b_{N-1}) \tag{2}$$

They form a two-dimensional sequence, C, which can be expressed as follows:

$$C = \begin{bmatrix} c_{00} & c_{01} & c_{02} & \cdots & c_{0,N-1} \\ c_{10} & c_{11} & c_{12} & \cdots & c_{1,N-1} \\ c_{20} & c_{21} & c_{22} & \cdots & c_{2,N-1} \\ & & & & \\ c_{M-1,0} & c_{M-1,1} & c_{M-1,2} & \cdots & c_{M-1,N-1} \end{bmatrix} \tag{3}$$

where $a_m, b_n, c_{ij} \in (0, 1)$

When M = N, sequence C can be obtained as follows:

$$c_{ij} = a_m \cdot b_n \tag{4}$$

$$\text{where, } m = p \cdot i + q \cdot j \pmod{M} \tag{5-1}$$
$$n = r \cdot i + s \cdot j \pmod{N} \tag{5-2}$$

The weight of this sequence, w_C, is equal to $w_A - w_B$. If it is assumed that the sequence vector of C is in the frequency axis direction and that the line vector is in the time axis direction, C can be regarded as a kind of frequency hopping pattern. Different sequences can be formed by cyclic shifting of one of the basic OOCs, A and B. Figure 1 shows examples of the formation sequence.

$$\begin{pmatrix} M = N = 5, w_A = w_B = 2 \\ A = (1\ 1\ 0\ 0\ 0) \\ B = (1\ 0\ 1\ 0\ 0) \\ \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 3 & 3 \end{bmatrix} \end{pmatrix}$$

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure 1 Sequence Formation Examples

3. Consideration of Correlation Characteristics

(1) Self-correlation characteristic

With the forming method described in the above section, the self-correlation characteristic of this sequence as the FH sequence becomes w_C at the sync point when the condition described below is met. It is 0 in other cases.

$$\begin{cases} M = N,\ w_c \le M \text{ when} \\ r = s = (M+1)/2, \\ p(\text{or } q) = (M+1)/2,\ q(\text{or } p) = (M-1)/2 \\ \text{where } \gcd(M,\ (M+1)/2) = 1 \end{cases} \tag{6}$$

(2) Cross-correlation characteristic

The maximum value of cross-correlation between sequences obtained by the cyclic shifting of one of the original sequences is as follows:

$$(\text{Max. cross-correlation}) \le \max\ (w_A,\ w_B) \tag{7}$$

4. Conclusion

We have proposed a method for forming code sequences for an FH communications system by extending the OOC in a two-dimensional manner and have examined its correlation characteristics. It may be necessary to develop a forming method that features better correlation characteristics and that can provide more sequences.

Acknowledgements

The authors express their gratitude to Assistant Professor Shin'ichi Tachigawa, Technical Officer Haruhide Hogari, and members of the Marubayashi Office of the university.

Part of this research was conducted with the help of a Scientific Research Expenses Subsidy from the Ministry of Education for General Research (A) "Research Into Spread-Spectrum Communications" (Subject No 6330203).

References

1. Chung, F.R.K., et al., "Optical Orthogonal Codes: Design, Analysis, and Applications," IEEE TRANS. ON IT, Vol 35 No 3, May 89, pp 595-604.

2. Miyagawa, Iwadare, and Imai, "Theory of Codes," Shokodo, 1978.

Control Channel Using SS-FH System in Mobile Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-360

[Article by A. Hirukawa, A. Kajiwara, and M. Nakagawa, Faculty of Science and Technology, Keio University]

[Text] **1. Introduction**

In mobile radio communications, control signals play a very important role in securing communications. In general, the control channel needs to be transmitted with a higher transmission quality than the quality required for speech signal transmission.

Focusing attention on the reliability of the control channel in mobile communications, this paper proposes a new communications control system using the FH (frequency hopping) technique, which can provide superior interference resistance than conventional systems, and evaluates the performance of this new system.

(2) Conventional Control Systems and a Control System Using FH Techniques

In conventional mobile communications, the control signals are transmitted through a specialized, narrow-band channel. With such a configuration, the control channel is very sensitive to the influence of interference waves, and, in the worst case, subsequent communications control can become impossible.

In contrast, the proposed system uses idle zones between existing channels and switches the carrier frequencies continuously (frequency hopping). This can reduce the influence of interference waves on the control signals. Also, the frequency diversity effect of FH is expected to improve fading, which is a major problem for mobile radios.

(3) Application of FH in Control Channel

Figure 1 is a conceptual diagram of the proposed system.

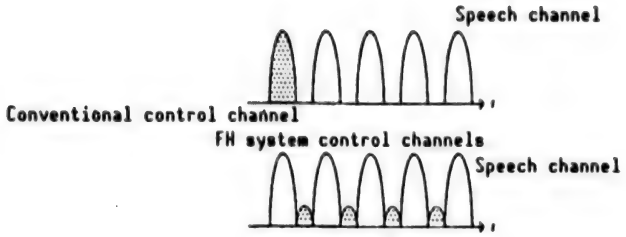


Figure 1. FH Conceptual Diagram

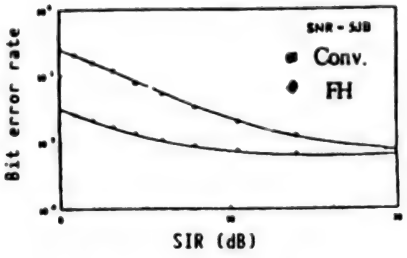


Figure 2.1 Relationship Between Strength of Interference Wave and Bit Error Rate

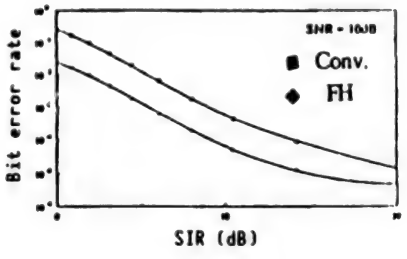


Figure 2.2 Relationship Between Strength of Interference Wave and Bit Error Rate

Carrier frequencies are placed at the centers of the guard zones between speech channels. Assuming that the information transfer rate of the control channel is "r" and that the carrier frequencies are switched for every "a" data item, the bandwidth, W_c, of the control channel per hopping is expressed as follows:

$$W_c = 1/ar \tag{1}$$

By assuming "a" so that its width can be accommodated in the guide zones between speech channels,and by selecting the center of each pair of speech channels as the carrier frequency, the interference between channels will consist only of the influence of side lobes.

(4) Bit ERror Rate

Evaluation of the bit error rate of the proposed system is as follows:

Assuming that one hop is performed per data item and that transmission is performed by means of two-phase PSK, the received signal becomes:

$$\begin{aligned} r(t) &= \cos(2\pi f_1 + a_i\pi) + N(t) + I(t) \\ N(t) &= n(t)\cos(2\pi f_1 + \phi_n(t)) \\ I(t) &= i(t)\cos(2\pi f_1 + \phi(t)) \end{aligned} \tag{2}$$

Where N(t) is the noise and I(t) the interference wave. When this signal is coherent-detected and only the low-frequency component is extracted, the signal becomes:

$$\begin{cases} r(t) = \cos(a_i\pi) + \hat{n}(t) + \hat{i}(t) \\ \hat{n}(t) = n(t)\cos(\phi(t)) \\ \hat{i}(t) = i(t)\cos(2\pi(f_c - f)t - \phi(t)) \end{cases} \quad (3)$$

Assuming a CW wave, the white noise of which is n(t), fc-fi is i(t), and $\phi i = \pi$, the probability density function of the demodulated data signal d(t) is of the Gaussian type.

While the interference wave continuously impacts on the signal in conventional systems, it is applied only once per h times in an FH system.

Based on the above, the bit error rate of a conventional system, $P_{e\ conv}$, can be expressed as follows:

$$p(x,m) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\{\frac{(-x-m)^2}{2\sigma^2}\}, \quad (4)$$

When

$$P_{e\ conv.} = \frac{1}{2} x \int_0^{-} p(x, I-1)\,dx + \int_{-}^{0} p(x, I+1)\,dx \quad (5)$$

Meanwhile, the bit error rate for the FH system, P_{eFH}, can be expressed as follows:

$$\begin{aligned} P_{eFH} = {} & \frac{1}{2}x\{\frac{1}{h}\int_0^{-} p(x, I-1)\,dx + \frac{h-1}{h}\int_0^{-} p(x,0)\,dx\} \\ & + \frac{1}{2}x\{\frac{1}{h}\int_{-}^{0} p(x, I+1)\,dx + \frac{h-1}{h}\int_{-}^{0} p(x,0)\,dx\} \end{aligned} \quad (6)$$

Here, the probability of the occurrence of marks and spaces is assumed to be 1/2.

5. Results of Calculations

In this case it is assumed that the CW waves of the carrier frequencies are applied as interference waves and that white noise is present.

It is also assumed that the control channels are digital, that frequency hopping occurs with every data point, and that the hopping count is 10.

If the FH is demodulated in an ideal manner, the bit error rate of the control channel is as shown in Figure 2. This result shows that the 10 hops can improve the bit error rate by about one-tenth.

6. Conclusion

This article proposes a method for applying FH in control channels and our research confirms that the proposed system can improve the bit error rate compared with conventional systems when CW interference is present.

Topics we plan to cover in future research include improving antifading performance and influence on speech channels.

Differential Despreading Method With Anti-Interference Circuit

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-390

[Article by A. Kajiwara and M. Nakagawa, Faculty of Science and Engineering, Keio University]

[Text] **1. Introduction**

This report proposes a code cycle division technique in which a different PN code repetition cycle is assigned to all stations using the same channel in a differential despreading system for DS-SS, together with a simplified circuit for the cancellation of narrow-band interference waves.

2. Systems and Characteristics

2.1 Code Cycle Division System

Code cycles that vary by one to a few clocks are assigned to the stations so that only the target station signal can be detected by means of differential despreading. Figure 1 shows the bit error rate for two cases, one in which several stations are positioned in a hexagonal pattern and a second where the stations are positioned in a square pattern around the target station. Here, it is assumed that the PN code sequence length is 127 bits, the SN ratio is -5 dB, the phases of the interference station carriers are random, and there are no narrow-band interference signals. Figure 1 shows that conventional differential despreading (Conv.) experiences strong interference from nearby stations, while the new code cycle division (New) that we propose can greatly improve reception quality. In particular, while reception is almost impossible to achieve with the conventional system when the interfering stations are near or when there are many of them, the use of the code cycle division technique makes it possible to improve reception quality greatly.

2.2 Narrow-Band Interference Canceler Circuit

This paper also proposes a new circuit for canceling narrow-band interference waves by taking advantage of the keen self-correlation characteristic of the PN codes. Figure 2 is a block diagram of a different-despreading demodulator

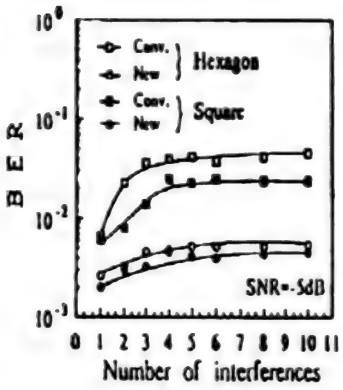


Figure 1. Relationship Between Number of Interfering Stations and Bit Error Rate

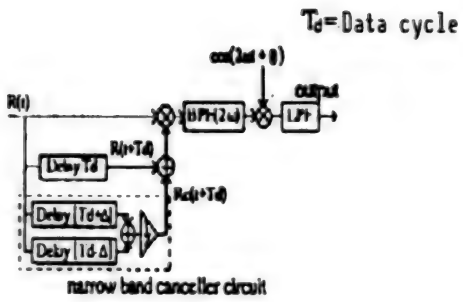


Figure 2. Block Diagram of Differential Despreader With Narrow-Band Interference Canceler Circuit

that incorporates this narrow-band interference canceler circuit. Figure 3 shows the relationship between BW_i/BW_d, the interference signal bandwidths normalized by information bandwidth BW_d, and the bit error rate. Here, the center frequencies of the interference waves are assumed to be the same as the SS signal carrier frequencies, and the code sequence length and SN ratio are the same as in 2.1 above, that is, 127 bits and -5 dB, respectively. Figure 4 shows the relationship between the number of interference waves and the bit error rate. Here, all of the SI ratios of the interference waves are assumed to be 0 dB, and their bandwidths, BW_i/BW_d, are 0.85, 1.27, 0.25, 3.2, 0.64, 5.2, 0.52, and 1.6, respectively. Figure 3 shows that the new system has considerably greater resistance to narrow-band interference than the conventional system, that the resistance is greater when the interference wave bandwidth, BW_i, is smaller, and that the narrow-band interference canceler circuit actually eliminates the influence of interference waves. In particular, when the SI ratio reaches -10 dB, the conventional system becomes almost incapable of reception because the bit error rate swells to about 0.5, but the new system, with its greatly improved characteristics, provides a bit error rate of 0.01. As this does not change when the number of narrow-band interference waves is larger, as shown in Figure 4, it can be demonstrated that a great improvement is possible even with multiple narrow-band interference waves.

3. Conclusion

Our research has demonstrated that code cycle division makes it possible to achieve multiplexing by differential despreading, which was generally thought to be almost impossible, and that this technique can ensure sufficient privacy. In addition, it has confirmed that merely adding a simple circuit produces a significant improvement in resistance to narrow-band interference waves when the center frequencies of interference waves are close to the carrier frequencies.

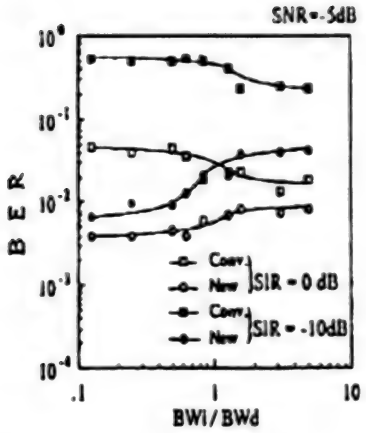


Figure 3. Relationship Between Normalized Interference Band and Bit Error Rate

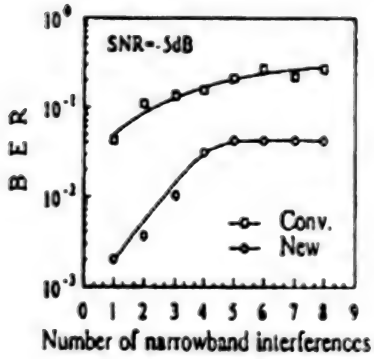


Figure 4. Relationship Between Number of Narrow-Band Interference Waves and Bit Error Rate

References

1. French, C.A and Gardner, W.A., "Spread-Spectrum Despreading Without the Code," IEEE TRANS. COMMUN., COM 34 No 4, 1986.

Application of Adaptive Canceler to Spread-Spectrum Communication System

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-392

[Article by H. Ohshima and T. Naito, Toyo Communication Equipment Company, Ltd.; and H. Niikura, Railway Technical Research Institute]

[Text] **1. Introduction**

The application of spread-spectrum (SS) communications in various fields has been examined over the last few years. Leakage coaxial cable (LCX) is suitable for SS communications because of its wide-band characteristics.[1] However, when a full duplex communications system is configured using code-division multiple access (CDMA) capability, it is difficult to separate the TX and RX signals of a UHF-band SS signal that share the same frequency band. This creates a relative distance problem due to the penetration of a signal transmitted from a station into its own receiver. This report deals with newly developed experimental equipment in which the principle of an adaptive noise canceler (ANC)[2] is applied as a countermeasure against this phenomenon.

2. Principle and Configuration

As shown in the concept diagram in Figure 1, the ANC cancels the noise component, n_0, in the input signal by subtracting signal y, which is obtained by applying complex weighting, W, to the reference signal, n_1, from the same noise source as the noise component, n_0, and from the noise component, n_0, contained in the input signal, and obtains only the required signal component, s. Figure 2 shows the circuit configuration of the experimental equipment. In this diagram, the circuit enclosed in broken lines corresponds to the ANC. This equipment uses the LMS algorithm, which minimizes the error power, as the W determination method. The correlation processing circuit is formed by a demodulator and an LPF, and W uses a variable-voltage PIN-ATT.

ϵ_2, the square of ϵ, which is the error signal containing the transmitted signal component that could not be canceled by the circuit shown in Figure 2, is expressed by the following equation:

$$\epsilon^2 = s^2 + (n_0-y)^2 + 2s(n_0-y) \quad (1)$$

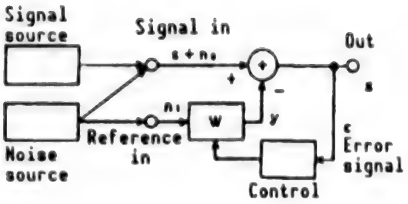


Figure 1. Principle of ANC

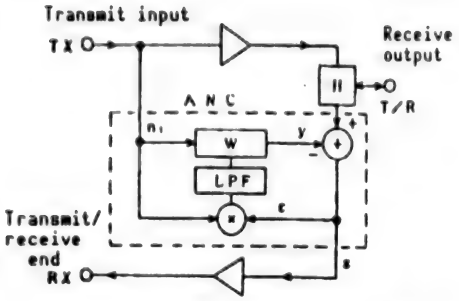


Figure 2. Configuration of Experimental Equipment

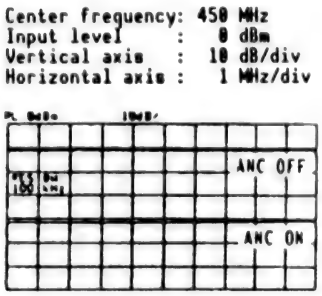


Figure 3. Receive Output Frequency Characteristic

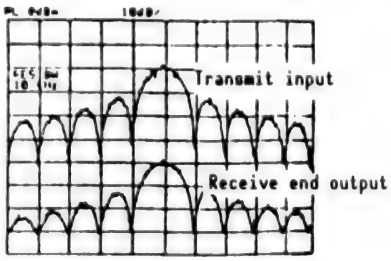


Figure 4. SS Signal Spectrum

Taking into account the fact that the SS communication system can be designed to minimize cross-correlation between the transmitted and received codes, s, corresponding to the received signal, and n_0, corresponding to the interfering transmitted signal, can be handled as signals with no mutual correlation. As s and y also have a similar relationship, when the expected value $E[\cdot]$ is assigned to each factor in equation (1) and the third factor $(2s(n_0-y)$ is assumed to be null, the equation becomes as follows:

$$E[\epsilon^2] = E[s^2] + E[n_e-y]^2] \qquad (2)$$

Because $E[s]^2$ is determined independently from W, the least mean square error (LMSE) in this system can be obtained as follows:

$$\min E[\epsilon^2] = E[s^2] + \min E[(n_0-y)^2]$$

Here, $E[(n_0-y)^2] = 0$ when $n_0 = y$. Also, under this condition, z is equal to s. Consequently, only the required signal is output.

3. Performance and Characteristics

Table 1 shows the main performance specifications of the equipment. Figure 3 shows the frequency characteristics of the transmit signal measured at the receiving end when a CW signal is input as the transmit signal. It shows that a suppression ratio of about 40 dB is achieved with ANC ON. Figure 4 shows the bandwidth characteristic measured using an SS signal with a spreading rate of 1 Mbps. A suppression ratio of more than 35 dB is obtained over a range of 10 MHz. The above measurements deal with the penetration of the transmit

signal; the receive signal is not input. For this reason, the measurements were made by connecting a coaxial terminator with a reflection loss of 40 dB or more to the transmit/receive end.

Table 1. Main Performance Specifications

Item	Performance specifications
Communications system	SS-DS
Modulation system	BPSK
Carrier frequency	450 MHz
Signal bandwidth	10 MHz
Suppression ratio	35 dB
Input level	0 dBm
Pass loss	±0 dB
Power consumption	500 mW
Dimensions	230 x 150 x 35 mm

4. Conclusion

This paper has described an experimental adaptive canceler device to be used in SS communications systems. Future research will include performance measurements from a more general point of view, such as the influence of the receive signal, and BER during CDMA.

References

1. Niikura and Sasaki, Proceedings of the Spring 1989 IEICE National Convention, SB-8-11.

2. Widrow, B., et al., PROC. IEEE., Vol 63 No 12, 1975 pp 1692-1716.

Application of Spread-Spectrum Communications System to Communications Cable

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-267

[Article by S. Ohira, K. Izawa, and L. Ishikawa, Tohoku Electric Power Company, Inc.; and A. Yokoi, M. Nishimoto, and T. Naito, Toyo Communication Equipment Company, Ltd.]

[Text] **1. Introduction**

Although optical fibers are being used in high-reliability, high-speed, and very high-capacity information communications systems associated with the electric power industry, conventional communication cables are still widely used in wired communications systems. One of the most promising methods for the effective utilization of existing communication cables is the specific surface (SS) communications system, which has several attractive features including code-division multiple access (CDMA) and only a small influence on other communications. This report consists of an examination, based on data obtained by actual measurements of the transmission characteristics of communication cables, into the relationship between the processing gain and transmittable distance when the SS communications system is used with communication cables.

2. Transmission Characteristics of Communication Cables

The communication cable (CPEV1.2) was originally designed for the transmission of signals up to a few hundred kilohertz, and its characteristics cannot be guaranteed at high frequencies. Therefore, the authors measured the transmission characteristics (attenuation constant α, phase constant β) up to 10 MHz. As a result, it has become clear that the attenuation constant, α increases almost proportionally to $\sqrt{f}$, while the phase constant, β, is almost proportional to f (Figure 1).

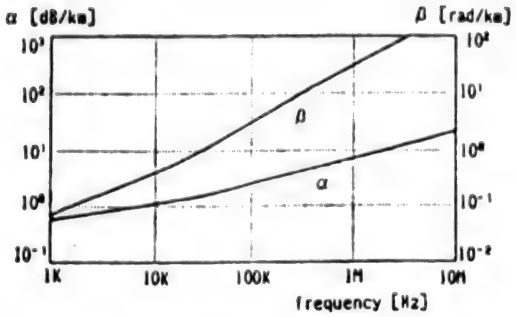


Figure 1. Transmission Characteristics of Communication Cable

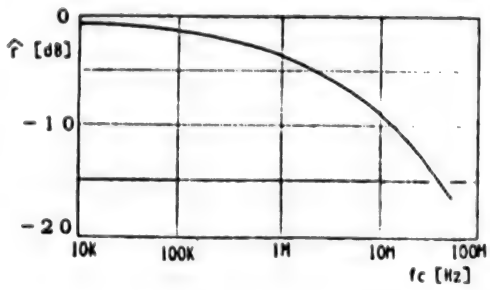


Figure 2. Degradation of Correlation Value $\hat{f}$

3. Degradation of Correlation Value Depending on Transmission Channel Characteristics

When spread code synchronization is assured between the transmitter and receiver, the correlation output, r, is equal to the total integrated value of the power spectrum density according to Percival's theorem.[1]

$$r = \int_{-\infty}^{\infty} S_{PN}(f)\,df \tag{1}$$

where $S_{PN}(f)$ is the power spectrum of the spread codes.

Assuming that the frequency characteristic of the transmission channel is H(f), the normalized correlation output after passing the transmission channel, $\hat{f}$, is as shown in the following equation:

$$\hat{f} = \int_{-\infty}^{\infty} S_{PN}(f)\,H(f)\,df \Big/ \int_{-\infty}^{\infty} S_{PN}(f)\,df \tag{2}$$

Figure 2 shows the $\hat{f}$ calculation result with respect to the spreading frequency, f_c. Due to the high-frequency attenuation characteristic of the transmission channel, the higher f_c, the more $\hat{f}$ is degraded. Consequently, it may be correct to think that simply increasing the processing gain, G_p, does not improve the system's performance.

4. Processing Gain and Transmittable Distance

This section deals with the transmittable distance, L, (maximum distance between transmitter and receiver that can provide a BER of no more than 10^{-4}) as one of the parameters for indicating the performance of an SS system. Assuming a model in which an interfering station having the same power as the target station is very close to the receiver (Figure 3), the results of calculating L as a function of G_p at information rates of 2,400 bps, 9,600 bps, and 36 kbps are shown in Figure 4.

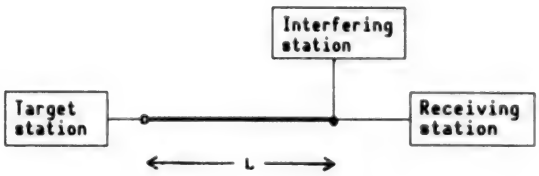


Figure 3. Transmission Model

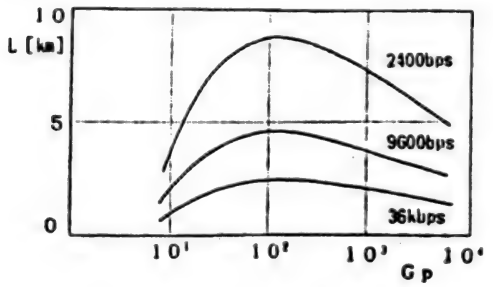


Figure 4. Transmittable Distance (L)

The results show that the effect of processing gain increase is present in the area where G_p is less than 10^2, but that L decreases due to the transmission channel characteristics when G_p is more than 10^2. It is also shown that L becomes flatter at higher information rates. Even so, the peak vale is attained when G_p is around 10^2, and thus the optimum value of G_p is around 10^2.

5. Conclusion

This paper has described the measurement of the transmission characteristics of a communication cable and the relationship between the processing gain and transmittable distance when the SS communications system is applied with a communication cable. Further experiments using the experimental equipment are scheduled for the future.

References

1. Tokoyama, M., "Spread-Spectrum Communication System," Kagaku Gijutsu Shuppansha, 1989.

Synchronization Method With SAW Matched Filter in VHF DS-SS System

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-268

[Article by H. Honda and M. Inatsu, Toyota Technological Institute]

[Text] **1. Introduction**

The spread-spectrum (SS) communications system has many advantages, including the reduced generation of interference, resistance to strong interference, and the possibility of code division multiple access communications. Nevertheless, stable acquisition of sync by the receiver is not easy because of the use of high-speed spread codes (PN codes). Also, simplification of the sync circuit poses an important problem that has to be solved. In our research, we produced an experimental VHF-band DS-SS communications system using a SAW matched filter in the sync circuit to simplify the circuit. In this circuit, a pulse train obtained from the matched filter and synchronized with the PN codes is used for forced locking of the phase of despreading PN codes, thereby making it possible to achieve stable synchronization and quick recovery from sync errors due to external causes. This report describes the results of an evaluation of the influence of the code-division multiplexed waves on the system.

2. Outline of Experimental System

Figure 1 shows the configuration of the experimental equipment, and Table 1 lists its specifications. For data transmitted by this system, a data bit is made to correspond to each PN code cycle. At the receiver, the output signal (peak value) of the matched filter, which can reduce the despreading PN code length from 127 in chip units, is first envelope-detected, then formed into pulses. The PN code length is reduced to provide a reset period, and the phase error is reset at each of these pulses.

3. Experimental Results

Figure 2 shows that it is possible to reduce the despreading PN code length. As the figure indicates, when the DU ratio is -5, the number of reducible limit chips that can maintain an error rate of 10^{-6} or better is 32. Based on this result and taking into consideration the interval required for resetting,

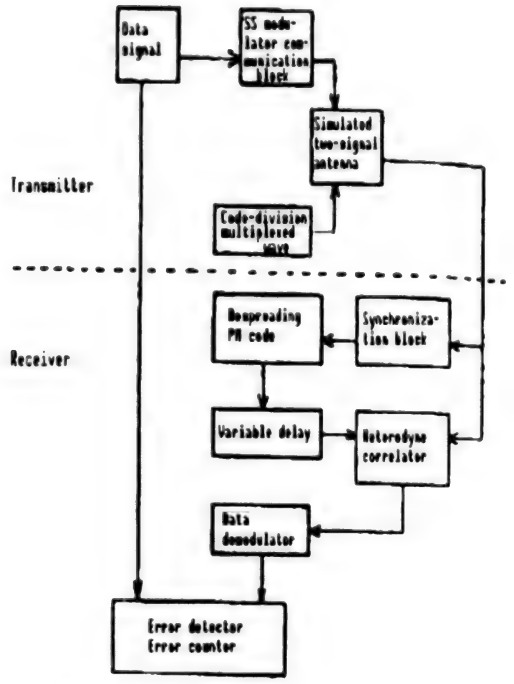


Figure 1. Outline of Experimental System

Table 1. Specifications of Experimental Equipment

Modulation system	Direct spreading
Carrier frequency	144 (MHz)
PN clock frequency	16 (MHz)
Spread bandwidth	32 (MHz)
PN code length	M sequence, 127 (chips)
Data transmission rate	126 (kbps)
Code-division multiplexed wave	127-chip DS-SS wave using M sequence of different patterns. (Carrier frequency is variable)

the chip count is set at 112. Figure 3 shows the DU ratio versus bit error rate characteristic with this code length, both under forced sync conditions and with this sync system. When this system is compared to the 127-chip forced sync method, it can be seen that the interference margin of the sync system is about 3 dB worse. However, as most of this is due to the low stability of the circuit, which converts the matched filter output into pulses, future improvements can be expected. When the error rate is measured using the center frequency of the multiplexed wave as a parameter, it was confirmed that the bit error rate can be improved if the interval of the multiplexed wave is more than the PN code clock frequency.

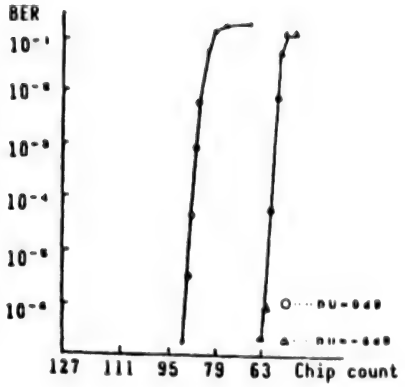


Figure 2. Despreading PN Code Length Vs. Bit Error Rate

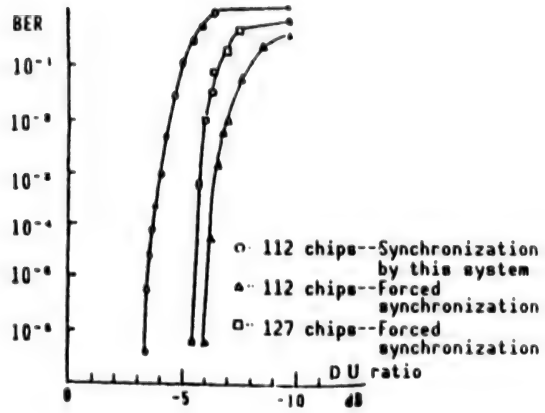


Figure 3. DU Ratio Vs. Bit Error Rate With Chip Count Reduced by 15

4. Conclusion

Experiments utilizing interference of multiplexed waves have demonstrated the basic characteristics of this synchronization system.

Note on Methods for Identifying Spread Codes for Spread-Spectrum Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-270

[Article by H. Fukumasa, R. Kohno, and H. Imai, Division of Electronic and Computer Engineering, Yokohama National University]

[Text] **1. Introduction**

Although it is necessary to understand the pseudonoise sequence [spread codes —translated by the source in this article as "pseudonoise sequence" in other articles this term is translated by the source as "spread codes"] to establish spread-spectrum (SS) communications and monitoring systems, not much research has been done on this point.

As the SS communications system transmits signals by spreading the bandwidth using pseudonoise sequences, the SS signal before despreading is very weak compared to the surrounding noise. Therefore, identification of pseudonoise sequences is almost the same problem as detecting an SS signal buried in the noise.

If the types of pseudonoise sequences for use as spreading codes can be limited, the SS signals can be determined by obtaining a correlation with each and every type of sequence, or can be reproduced utilizing the properties of the sequences. (The paper cited in Reference 1 describes the use of the properties of the LFSR sequence.)

However, if the presence of other transmitters is assumed, these methods are not valid because the types of pseudonoise sequence cannot be limited. In this case, the receiver may be able to prepare several sequences and determine the range of the pseudonoise sequence for the correlation values between the prepared sequences and the input signals, or to directly synthesize codes having good correlation with the pseudonoise sequence. However, these methods still involve a number of problems, for example, the kind of sequences to be prepared on the receiver side.

This report proposes a method for identifying two-dimensional pseudonoise sequences, of types which are not specified, from the received signal buried in noise. This is based on the assumption that the cycle of the pseudonoise sequence is known.

2. Pseudonoise Sequence Identification Method

In the following, the SS modulation used is assumed to be direct-speed (DS) modulation. The basic principle of the proposed method is to detect whether the successive chips of the pseudonoise sequence are reversed or not, and to identify pseudonoise sequences from this information. In normal SS communications, the spectrum is spread by assigning a few cycles of pseudonoise sequences per data bit. This is based on an inherent property of SS signals—the fact that there is a probability of one-half that the pseudonoise sequence codes will be reversed at every cycle. Therefore, if simple sync addition is performed at every cycle, it may be very difficult to eliminate the influence of noise as well as to identify pseudonoise sequences, because the information they carry is also canceled.

To solve this problem, it may be possible to improve noise canceling by sync addition to make it suitable for use in the identification of pseudonoise sequences in SS communications. In other words, a differential pulse is generated between each pair of pseudonoise sequence chips and is used in judging whether the chips are reversed or not. By sync addition of these pulses, the influence of noise can be reduced and the features of the pseudonoise sequences can be exploited more fully.

Here, communication channel noise ignores spread signals from other stations caused by code-division multiplexing, but refers only to Gaussian noise caused by P_N spreading. The signal is assumed to be (+1, -1), and the cycle, n, of the pseudonoise sequence is assumed to be known. When detecting the reversal of successive chips, the product of successive chips is calculated. The presence of reversal is detected when the product is negative, the absence of reversal is detected when it is positive, and a hard judgment is made as to (+1, -1). To reduce the influence of noise on the judgment, the judgment results are sync-added cyclically. Hereafter, the result of the hard judgment of the product of successive chips is referred to as the reversed sign.

Example:

> When data (1, 1, -1) are superimposed on a pseudonoise sequence (1, 1, -1, -1, -1, 1, -1), the input signal I and reversed signs, R, are as follows:
>
> I: (1,1,-1,-1,-1,1,-1,1,1,-1,-1,-1,1,-1,-1,-1,1,1,1,-1,1)
> R: (1,-1,1,1,-1,-1,-1,1,-1,1,1,-1,-1,1,1,-1,1,1,-1,-1)
>
> The sequence is reproduced by applying reversals between negative reversed signs.

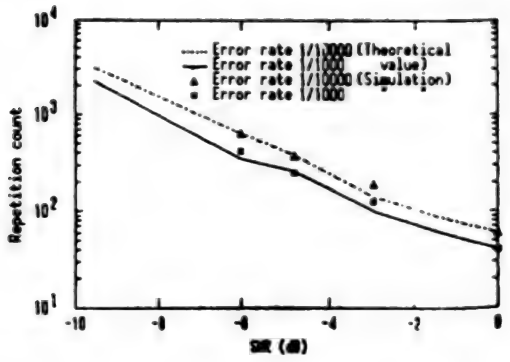


Figure 1. S/N Ratio Providing Constant Bit Error Rate Vs. Repetition Count

3. Theoretical Value of Bit Error Rate and Results of Simulation

When sync addition is to be applied on the reversed signs over M cycles, the probability that the sum is erroneous due to the effect of noise can be obtained from the following formula:

$$\sum_{r=0}^{M/2} \binom{M}{r} (0.5 + 2p(\frac{1}{\sqrt{P_N}})^2)^r (0.5 - 2p(\frac{1}{\sqrt{P_N}})^2)^{M-r}$$

where $p(z) = \frac{1}{\sqrt{2\pi}} \int_0^z e^{\frac{x^2}{2}} dx$

Figure 1 shows the relationship between the signal to noise ratio (S/N) repetition count when the probability that a reversal sign bit is erroneous is within the target value (10^{-3} and 10^{-4}).

As shown above, the influence of noise can be suppressed by sync addition. However, as there are reversals according to the data between the first chip and last chip in a sequence, the reversed sign is either positive or negative with a probability of one-half. Assuming that the reversed signs are correct except for the start and end of data, one of the following two cases occurs with the same probability:

1. In the case where there is an even number of reversed signs: pseudonoise sequence can be obtained as it is.

2. In the case where there is an odd number of reversed signs: the reproduced sequence is a sequence with 2n cycles. This consists of the pseudonoise sequence and its reversed sequence.

In either case, synchronization with the input signal is acquired so despreading can be performed directly. In the second case, the despread data differs from the transmitted data. But if the boundary of the data can be found by despreading, the pseudonoise sequence can be obtained by dividing the generated sequence with 2n cycles at the boundary to obtain a sequence with n cycles.

4. Conclusion

The proposed method can perform the despreading of SS signals even when the pseudonoise sequence is unknown and the signal is buried in noise, provided only that the cycle is known. This makes it possible to determine the transmission power required for the control of the communications station and also to understand the communications station itself. For actual implementation in the future, examinations into the effects of interfering stations and identifying measures to apply in case the cycle is unknown or if code-division multiplexing is applied will be necessary.

References

1. Yokoyama, M., "Method and Equipment for Monitoring Spread-Spectrum Signal Stations," PATENT REPORT, (B2), A-8226-5K, 1988-31128.

Verifiable Public Distributed Sum Protocol

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-281

[Article by K. Kobayashi and K. Tamura, Yamagata University; and Y. Nemoto, Tohoku University]

[Text] **1. Introduction**

The problems presented by distributed sum[1] and vote protocols are two fields of public key cryptography where research has been more active than ever in recent years. For the distributed sum protocol, some users have their own individual secret values, each of the users tells only a fragment of his or her secret value without uncovering the whole, and the protocol is used to obtain the sum of the fragments told by all users. When the secret values consist only of 0's and 1's, this protocol can also be used as a voting protocol.[1] This report proposes a simplified distributed sum protocol that can be used to obtain the sum of the secret values told by the users without secret communications, and that can check for an illegal presence during the calculation of the subtotals.

2. Protocol

The conditions for use of a bulletin board are as follows: Users, U_i, the number of which is m ($1 \leq i \leq m$), are connected to the bulletin board. Each of the users has his or her own area in the bulletin board. He or she can write only in his or her area, but any user can read all areas freely.[1]

- **Phase 1: Key Generation**

  First, a large prime number, p, is selected. Next, two secret keys, x_i and $x_{i+1} \in [1,p-1]$ $(i=1,\cdots,m)$, are determined for user U_i. Here, it is assumed that $x_{m+1} = x_1$.

- **Phase 2: Disassembly**

  Each user U_i disassembles, in a random manner and using the secret keys, his or her own secret value $S_i \in [0,p-1]$ into two fragments, $S_{i,i}$ and $S_{i,i+1} \in [1,p-1]$, which meet the following condition:

  $$S = S_{i,i} + S_{i,i+1} X_{i+1} \bmod p \tag{1}$$

  Here, $S_{m,m+1} = S_{m,1}$. One such disassembly technique is to determine the value of $S_{i,i}$ arbitrarily and to obtain the value of $S_{i,i+1}$ so that it can satisfy formula (1).

- **Phase 3: Bulletin**

  Each U_i displays the created $S_{i,i}$ and $S_{i,i+1}$ horizontally on the bulletin board.

- **Phase 4: Subtotal**

  Using the secret key, x_j, each U_j and U_{j-1} ($j=1, \cdots, m$) calculates the subtotal in the vertical direction, as shown below, and displays this value individually on the bulletin board again:

  $$t_j = (S_{j-1,j} + S_{j,j})\, x_j \bmod p \tag{2}$$

  Here, it is assumed that $U_0 = U_m$ and that $S_{0,1} = S_{m,1}$.

- **Phase 5: Checking**

  The presence of an illegal entity is checked based on whether the two subtotal values t_j obtained in Phase 4 coincide or not. It is judged that there is no illegal presence when the two values for t_j coincide. When they do not coincide, a secret key, x_j, is made public to identify the illegal user. If three secret keys are identified for each user, and the secret value S_i is disassembled into three fragments in Phases 1 and 2, three users calculate a subtotal, t_j, and display it on the bulletin board; in this case, the illegal user can be determined by majority rule, without making the secret key, x_j, public.

- **Phase 6: Sum**

  Each user can obtain the sum of S_i by adding all subtotal values t_j:

  $$T = \sum_{j=1}^{m} t_j \bmod p \tag{3}$$

Figure 1 shows the process of executing the proposed protocol.

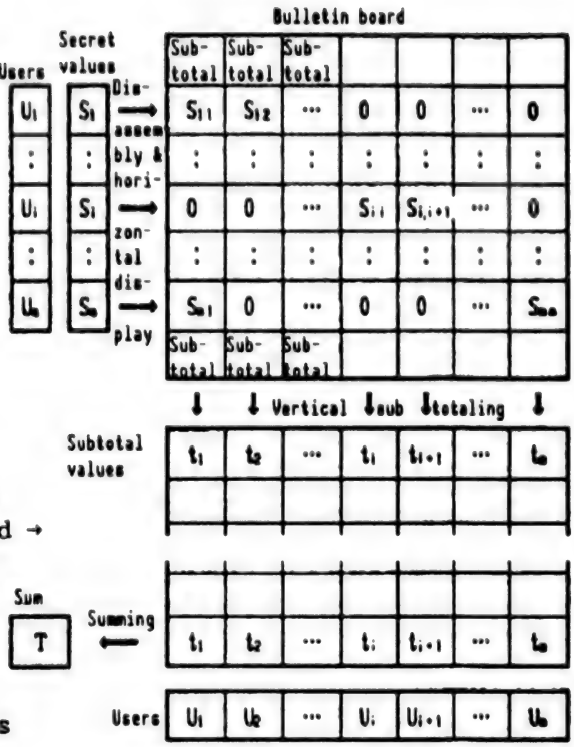


Figure 1. Execution Process for Proposed → Protocol

3. Example of Values

Assume the following values: p = 101, the number of users is 5; the secret keys are $x_1 = 19$, $x_2 = 82$, $x_3 = 37$, $x_4 = 65$, and $x_5 = 43$ (each user has two secret keys); and the secret values of the users re $S_1 = 1$, $S_2 = 0$, $S_3 = 1$, $S_4 = 0$, and $S_5 = 1$. The secret values are disassembled into the following fragments, which are displayed on the bulletin board:

$$S_1 = 1 \rightarrow 54\ x_1 + 38\ x_2, \qquad S_2 = 0 \rightarrow 91\ x_2 + 44\ x_3$$
$$S_3 = 1 \rightarrow 23\ x_3 + 18\ x_4, \qquad S_4 = 0 \rightarrow 76\ x_4 + 19\ x_5$$
$$S_6 = 1 \rightarrow 68\ x_5 + 96\ x_1$$

Then, each user calculates t_j in formula (2) using his or her two secret keys, and obtains the following results; $t_1 = 22$, $t_2 = 74$, $t_3 = 55$, $t_4 = 50$, and $t_5 = 4$. The value obtained by displaying them on the bulletin board again and summing them is T = 3.

4. Conclusion

The advantages of the proposed protocol are that it can obtain the sum of the secret values of the users without secret communications, and that it is possible to check for the presence of an illegal entity when calculating the subtotals. However, this protocol also has a disadvantage, which is that it is vulnerable to conspiracy. If two users, U_{i-1} and U_{i+1}, conspire, the secret values for S_i of user U_i can easily be found by users U_{i-1} and U_{i+1}.

References

1. Masumoto, Y., Matsumoto, T., and Imai, H., "Distributed Sum Protocol Based on Distributed Logarithm Problem," CIS '89, Feb 1989.

IC Card for Key Predistribution System, Cryptographic Communications

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-282

[Article by T. Matsumoto, Y. Takashima, and H. Imai, Division of Electronic and Computer Engineering, Yokohama National University; and M. Sasaki, H. Yoshikawa, and S. Watanabe, Delta A Laboratories, ADVANCE Company, Ltd.]

[Text] **1. Introduction**

This report deals with KPSL1CARD, a prototype of a KPS (key predistribution system) card. Such cards play an important role in building a cryptographic communications system for use in large-scale networks capable of sending encrypted messages in mail format to a specified entity subscribing to the system. KPSL1CARD is an IC card which has a cryptographic key predistribution function based on the KPS linear scheme,[1] a random number generation function, a cryptographic communications function based on DES, and a file management function. KPSL1CARD is used in connection with a KPS adapter that is compatible with the communications medium used (facsimile, personal computer communication...). The prototype was developed in order to examine the possibility of implementing KPS based on a linear scheme.

2. KPSL1CARD[3]

Figure 1 shows the external configuration of KPSL1CARD, while Figure 2 shows its internal configuration. The prototype we have developed integrates a considerable number of components to ensure multifunctionality and a high degree of safety, but it is expected that the KPS linear scheme can be implemented using more simplified IC cards in the future. The number of KPSL1CARD chips can also be reduced by the use of application-specific LSIs.

3. Cryptographic Communications System Using KPSL1CARD

Figure 3 shows an example of a cryptographic communications system using KPSL1CARD. This example is for facsimile communications, but cryptographic communications can also be implemented for other communications media by using a KPS adapter compatible with each medium. The cryptographic processing is not done by the KPS adapter, but the whole process is performed within KPSL1CARD.

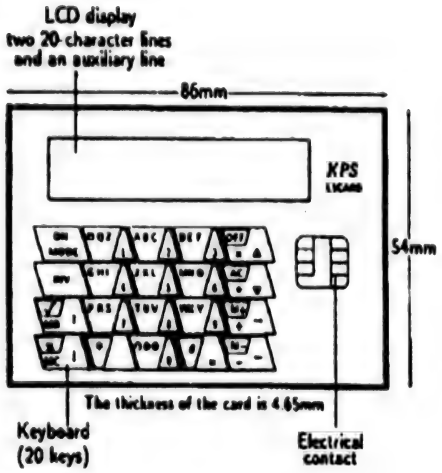


Figure 1. External Configuration of KPSL1CARD

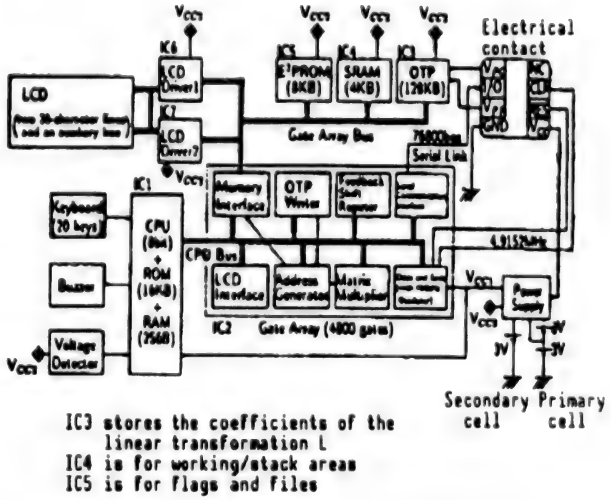


Figure 2. Internal Configuration of KPSL1CARD

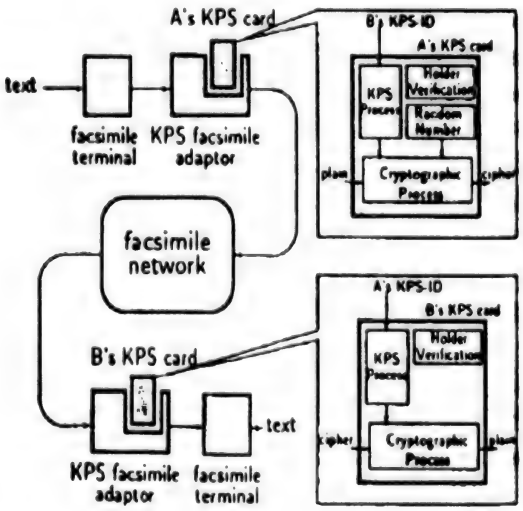


Figure 3. Example of Cryptographic Communications System Using KPSL1CARD Cards

Utilizing the CBC DES mode, the output from the random number generator in the card is used as the work key, and the output from the secret KPS algorithm is used as the master key. The whole of DES is implemented by software. Cryptographic communications, including interfacing with the adapter, can be performed at a rate of 4,800 bits/second or higher.

The keys are predistributed based on the linear scheme, which is one of the techniques of KPS, and are processed inside KPSL1CARD. When the address KPS-ID (512 bits) is input via the keyboard on the card or from a file (or the adapter), KPSL1CARD computes the common key automatically according to the secret algorithm of the linear scheme. This computation consists of two parts

—the ID transformation algorithm[1] and linear transformation part. The former is implemented by software[1] and the latter is implemented by hardware. The whole of the key predistribution process is completed in no more than 0.7 seconds. The data for the linear transformation part are generated by (one or two) KPS centers (management organs) at the time the KPS card is issued based on the KPS-ID of the KPS card holder and the secret data of the KPS centers. The data are recorded onto the KPS card in such a way that no one can read it from the KPS card. Even if the data in the linear transformation part of a KPS card is read out by chance, the security of other subscribers will not be impaired unless the same action is carried out successfully on at least 8,191 other KPS cards.

In addition, KPSL1CARD has a holder verification function based on passwords, a card lock function for locking itself in case of illegal use, a log function for storing card operation records, an information directory function (telephone directory and KPS-ID directory), and a calculator function.

4. Conclusion

A prototype IC card, KPSL1CARD, was developed to implement key predistribution and cryptographic communications. The prototype has provided us with the prospect of implementing the KPS linear scheme using current technologies.

References

1. Matsumoto and Imai, "Technique of Distributing Cryptographic Keys Without Communications: Key Predistribution System," TRANSACTIONS OF IEICE, Vol J71-A No 11, Nov 88, pp 2046-2053.

2. Matsumoto, Takashima, and Imai, "Configuration of a Simplified ID-Transformation One-Way Algorithm," IEICE NEWS, IT89-23, Jul 89.

3. Matsumoto, T., et al., "The KPS Card—IC Card for Cryptographic Communications Based on the Key Predistribution System," Smart Card 2000, Oct 89.

One-Way Key Distribution System Based on Identification Information Without Public Information Directory

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-283

[Article by T. Itoh, T. Habutsu, I. Sasase, and S. Mori, School of Science and Engineering, Keio University]

[Text] **1. Introduction**

In recent years, many proposals have been made with regard to key predistribution systems with an identification function based on ID information. Representative examples are described in the papers cited in references 1 and 2. The former system features easy, direct identification and a relatively simple design. But it requires two-way communications and can predistribute keys between only two users. In contrast, the latter system uses one-way communications but requires a public information directory. Therefore, by combining the advantages of these two systems with the advantage of the system described in reference 4 which uses Schalkwijk's algorithm described in reference 3, this report proposes a one-way key distribution system that can generate common keys based on ID information for multiple users without using a public information directory.

2. One-Way Key Distribution System Based on ID Information

The proposed key distribution system assumes that there is a reliable center.

2.1 Center Algorithm

Step 1: Generates two large prime numbers, p and q; assumes that $N = p \cdot q$; and computes e, d, $\overline{ID_i}$, k_i, and $\overline{k_i}$ so that these values meet the following conditions:

$$e \cdot d = 1 \pmod{L}$$
$$ID_i \cdot \overline{ID_i} = 1 \pmod{L}$$
$$k_i \cdot \overline{k_i} = 1 \pmod{L}$$

where L = 1 cm (p-1, q-1)

Step 2: Computes s_i and u_i so that they meet the following conditions:

$$s_i = ID_i^{-d} \pmod{N}$$
$$u_i = \overline{k_i} \cdot d \cdot \overline{ID_i} \pmod{L}$$

Step 3: Using Schalkwijk's algorithm, expresses the ID information (integer ID_i) as an n-dimensional two-level vector with hamming weight w as follows:

$$ID_i = (a_1, \cdots, a_n) \quad a_m \in GF(2)$$

Also, defines the index set of ID_i, I_i, as follows:

$$I_i = \{m | a_m = 1, 1 \le m \le n\}$$

Step 4: Generates n-dimensional vector

$$X = (x_1, \cdots, x_n)$$

which can meet the following condition:

$$k_i = \sum_{m \in I_i}^{n} x_m$$

and computes the following:

$$G = (g^{x1}, \cdots, g^{xn})$$

where g is the primitive root of GF(p), GF(q).

Then, stores (ID, N, e, g, s_i, u_i, G) in the IC card and hands it to user i.

2.2 Key Generation Algorithm

The following description assumes communications from user i to user j.

Step 1: User i generates a random number, r_i, and computes the following:

$$K_y = g^{ri} \pmod{N}$$

and maintains its secrecy.

Step 2: User i computes the following using the ID information of user j:

$$t_j = \prod_{m \in I_j}^{n} G \cdot ID_j = g^{\sum_{m \in I_j}^{n} m} \pmod{N}$$

Step 3: User i transmits the following to user j:

$$x_{ij} = s_i \cdot t_j^{r_i ID_j} \quad (\text{mod } N)$$
$$y_{ij} = t_j^{r_i \bullet ID_j} \quad (\text{mod } N)$$

Step 4: User j identifies that the transmitter is user i based on the following:

$$y_{ij}/x_{ij}^{e} = ID_i \quad (\text{mod } N)$$

and computes common key K_y.

Since the created key depends only on r_i, the same key can be distributed to other users by the same method so key predistribution to multiple users is possible.

3. Conclusion

This report proposes a one-way key distribution system based on ID information that does not use a public information directory and that can generate a common key even among multiple users. Themes for the future may include reducing the burden of generating secret information by the center, functions, etc.

References

1. Okamoto and Tanaka, "Proposal for Cryptographic Key Distribution System Based on Identification Information," IEICE TRANSACTION (D), J72-D, Vol 11, Apr 89, pp 293-300.

2. Tanaka and Okamoto, "One-Way Key Distribution System Based on Identification-Related Information, IEICE NEWS, ISEC 89-3, May 89.

3. Schalkwijk, J.P., "An Algorithm for Source Coding," IEEE TRANS. INFOR. THEORY, Vol IT-18 No 3, May 72, pp 395-399.

4. Tanaka, H., "Cryptography System Based on Identification Information Implemented by Comparison of Information Between Two Layers," 12th Symposium on Information Theory and Its Applications, Dec 89.

Implementation of High-Speed Modular Exponentiation Calculator

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-284

[Article by T. Hasebe, N. Torii, M. Azuma, and R. Akiyama, Fujitsu Laboratories, Ltd.]

[Text] **1. Introduction**

RSA cryptography[1] using modular exponentiation calculation $R = M^E \bmod n$ as the encryption function has been established as a safe public key cryptography system. However, as n should be 512 bits or more to ensure sufficient safety, a vast number of calculations is required, thereby making it essential to increase the computation speed. Therefore, the authors propose a high-speed computation method using a modular table.[2] However, this system uses a parallel processing configuration. the hardware for such a system would have to be large and division for implementation in an LSI is complicated.

This report proposes a modular exponentiation calculator with smaller hardware for the basic configuration and with excellent extendibility that allows higher-speed processing when required. The calculator is capable of modular multiplication as the basic operation for modular exponentiation as well as multiplication, addition, and modular computations of multiple digits.

The authors manufactured a prototype of the modular exponentiation calculator, which is also described in this report.

2. Modular Exponentiation Computation Algorithm

Modular exponentiation is performed by repeating modular exponentiation calculation according to a high-speed exponentiation algorithm. The following description refers to a case in which 512-bit modular multiplication A x B (mod n) is performed with a processing unit of 32 bits. When divided into 32-bit units, B can be expressed as shown in formula (1) below:

$$B = B_{15} \times 2^{480} + B_{14} \times 2^{448} + \cdots + B_1 \times 2^{32} + Bo \quad (1)$$

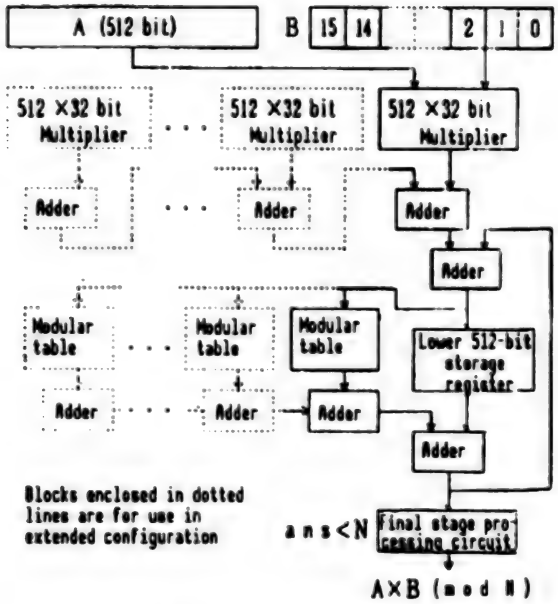


Figure 1. Block Diagram of Prototype

The value of the modular multiplication can be expressed in formula (2) below using partial products M_i ($=A \times B_i$):

$$A \times B \pmod{n} = \quad (2)$$
$$(\cdots(((M_{15} \pmod{n} \times 2^{32}) + M_{14}) \pmod{n} \times 2^{32}) \cdots + Mo) \pmod{n}$$

The calculator is designed to obtain the modulus of the partial products in accordance with formula (2), except that the intermediate calculations for modular computations do not limit the modular results to less than n, and the result is limited to less than n only at the final stage processing circuit. When the calculator is extended, the unit of division for formulas (1) and (2) becomes 64, 128, 256, or 512 according to the number of parallel processors.

3. Configuration of Prototype

Figure 1 shows the configuration of the prototype (blocks enclosed in dotted lines are extended circuits). The processing is performed in 32-bit units, and the adder is a 32-bit adder. The basic configuration is composed of a multiplier circuit and a modular table. Multiplier circuits and modular tables are added for extension. The numbers for both of them are 16 in the case of 16-parallel extension. As for the operation, a partial product is first calculated by the multiplier circuit and output from the bottom word. The lower 512 bits are stored in the register and the bits above 512 bits are sent to the modular table for retrieval. The output from the modular table is added to the lower 512 bits to obtain the intermediate modular computation result. This result is then added to the next partial product to compute the modulus again, and this computation is repeated to obtain the intermediate modulus of A x B (mod n). Ultimately, the final result is obtained by limiting the result to less than n according to the value of the intermediate modulus at the

processing circuit in the final stage. In the case of an extended configuration, several partial products are calculated in parallel, and they are added to obtain extended partial products. Due to the increase of the number of bits in the partial products, the modular table is also extended and several tables are retrieved in parallel.

The prototype is composed of four circuit boards (board size: 500 x 382 mm). These are the control board, the modular computation board, the multiplication board (with 4 circuits), and the modular table board (with 2 circuits). These four PC boards are the basic configuration. An additional 14 PC boards can be used to implement a 16-parallel extended configuration.

4. Conclusion

The authors proposed and manufactured a prototype of a modular exponentiation calculator with good extendibility. When 512-bit RSA encryption processing is performed on the prototype using a 10 MHz clock, the average throughput obtained is 12.2 kbps, confirming the validity of the basic configuration. As for the implementation in LSIs, the use of a fully formed OMS gate array provides the prospect of implementation using two chips (approximately 35,000 gates + 90K RAM). If the LSIs use a 30 MHz clock, the throughput would reach 36 kbps, with the basic configuration, and 360 kbps with a 16-parallel extended configuration, which would make the LSIs compatible with various applications for modular multiplication. Table 1 shows the results of an examination of implementation in LSIs. Plans for the future include examining prospects for implementation as well as the development of applications for key management, signature, etc., by using a network to which the prototype is connected.

Table 1. Relationship Between Configurations, Hardware Scales, and Average Throughput (When implemented in LSIs)

Configuration	1-parallel	2-parallel	4-parallel	8-parallel	16-parallel
Logic (gate)	35,000	53,000	89,000	161,000	305,000
RAM (kbits)	90	157	282	538	1,050
Throughput (kbps)	36.6	(66)	(114)	(159)	*(366)

Values inside ( ) are estimates.
Value marked * is for pipeline processing.

References

1. Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signature and Public Key Cryptosystem," CACM, 21 Feb 78.

2. Torii, Azuma, and Akiyama, "Configuration of RSA High-Speed Parallel Multiplication/Division LSI," 1987 IEICE National Convention, Mar 87.

Modular Exponentiation Method Using Fast Constant Multiplication Algorithm

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-285

[Article by K. Takabayashi, S. Kawamura, and A. Shinbo, Toshiba R&D Center]

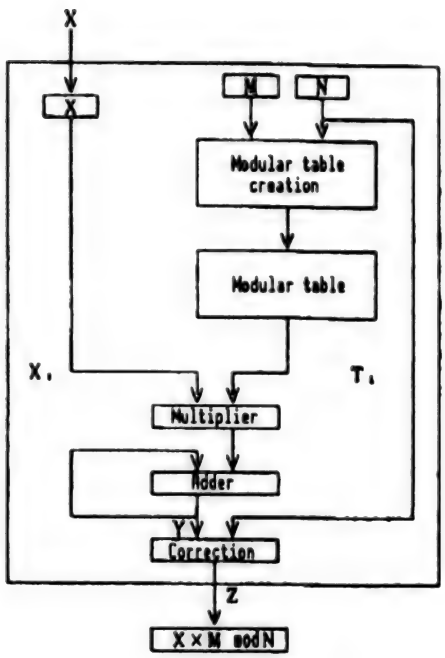
[Text] **1. Introduction**

The RSA cryptography and public key distribution systems often use modular exponentiation of multiple-length integral numbers, M^E mod N, but this operation presents an obstacle to implementation due to the huge number of calculations required. Some methods which use modular tables to increase the modular computation speed have been proposed, and all of them make use of the fact that a divisor, N, can be regarded as a constant.[1] However, when a fast exponentiation computation technique processes exponents from the higher bits, approximately one-third of the repeatedly executed modular multiplications are constant-multiplication modular computations. Here, constant-multiplication modular computation refers to the case in which M in a modular multiplication M x X mod N is a constant. This report proposes a new table reference method by utilizing the fact that in constant-multiplication modular computation, not only the divisor, N, but also the multiplier, M, can be incorporated into the table.

2. Constant-Multiplication Modular Computation by Means of Table Reference

In the following description, M, N, and X are assumed to be 512-bit integers. Assuming that the intermediate variable is X, the modular exponentiation can be disassembled into repetitions of X x X mod N and M x X mod N. The ratio of the frequency of the appearances of these calculations is 2:1 on average. With the latter calculation, which is a constant-multiplication modular computation since M and N can be regarded as constants, the result of the modular multiplication can be obtained directly from X and the modular table created from M and N.

First, the q-level development of the intermediate variable, X, is expressed as follows:



← Figure 1. Constant-Multiplication With Modular Computation

$$X = \sum_{i=0}^{l} X_i \cdot q^i \qquad (1)$$

(where $0 \leq X_i \leq q-1$)

Then, M x X mod N can be calculated in steps (1) to (4) below. The use of an algorithm for constant-multiplication modular computation is shown in Figure 1).

(1) Acquire modulus T_i from M and N, and save it in the memory.

$$T_i = M \times q^i \mod N \quad (0 \leq i \leq \ell) \qquad (2)$$

(2) Compute congruent value Y with divisor N from result Z with the following formula:

$$Y = \sum_{i=0}^{l} X_i \times T_i \qquad (3)$$

(3) From Z = Y mod N, correct Y and output Z.

(4) Repeat steps (2) and (3) for a new X.

If the number of repetitions is sufficiently large, the time required for processing steps (2) and (3) will be dominant. The correction in step (3) is easier than the computation in step (2), as the number of calculations required for formula (3) is almost equal to a multiple-length multiplication computation.

3. Processing Time

The following description deals with the processing time required when the proposed method is applied to the execution of modular exponentiation computations. There are two methods for implementing the constant multiplication parts in modular exponentiation, as follows:

Method 1 (Processing time T_1): Implementation by multiplication and modular computations

Method 2 (Processing time T_2): Implementation by constant-multiplication modular table

Assume that the number of bits in exponent E is m, the hamming weight is m/2, the table creation time and the time required for other preprocessing operations can be ignored, and that t_1, t_2, and t_3 are as follows:

t_1: Multiplication processing time
t_2: Modular computation processing time
t_3: Modular multiplication (proposed method) processing time

Now, the ratio between T_1 and T_2, r, can be expressed as follows:

$$r = T_2/T_1 = \frac{m(t1+t2) + (m/2)\,t3}{m(t1+t2) + (m/2)(t1+t2)} \qquad (4)$$

Here, if it is assumed that $t_1 = t_2 = t_3$, then r is equal to 5/6, which translates into a reduction of processing time of approximately 17 percent. Under this assumption, the time required for the constant-multiplication modular computation alone is reduced by one-half.

As for the processing performance of modular exponentiation computations using 16-bit fixed-point DSP (performance: 40 MIPS) by applying the above constant-multiplication modular computation algorithm, throughput with a 512-bit divisor will be approximately 4 kbps.

4. Conclusion

This report proposes a constant-multiplication modular computation algorithm which uses a modular table to execute the constant-multiplication part of modular exponentiation in approximately the same processing time as the multiplication time. The proposed method allows the exponentiation multiplication processing time to be reduced by approximately 17 percent.

References

1. Tanaka and Okamoto, "Modular Exponentiation Using Signal Processor," 1987 National Convention of the IEICE Information and Systems Department.

Factorization Attack Against Some Acceleration Protocols for RSA Secret Transformation

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-286

[Article by A. Shimbo and S. Kawamura, Toshiba Research and Development Center]

[Text] **1. Introduction**

Methods for performing the secret transformations required for RSA cryptography by accelerating computations have been examined (see references 1, 2, 3, 4, as well as other papers). This report demonstrates that some of the acceleration protocols that have been proposed to date involve the possibility of exposing the client's secret information by an illegal operation of the server who is undertaking the computations, and considers some countermeasures to prevent this.

2. Factorization Misusing Acceleration Protocols

This paper deals with two acceleration protocols that can be vulnerable to the attacks described above. These are the RSA-S2 protocol[1] and the KS2 protocol.[2] The following describes the method by which the server can attack the KS2 protocol, but the same procedure can also be used with the S2 protocol.

Presuppositions

(1) The server is capable of understanding a plain message, M, commissioned by the client.

(2) The server is capable of knowing the commissioned computation result, S.

Here, to simplify discussion, it is assumed that S is not checked (or that S passes checking). Except for this assumption on checking, the presupposition above generally holds true.

Factorization misusing KS2 protocol

(1) The client divides the secret key, d, as follows:

$$d = d_{cp} + \Sigma_i f_i d_i \quad \text{mod } p-1$$
$$d = d_{cq} + \Sigma_i g_i d_i \quad \text{mod } q-1$$

Assume that $D_s = [d_1, d_2, \cdots, d_m]$,
$F = [f_1, f_2, \cdots, f_m]$, and
$G = [g_1, g_2, \cdots, g_m]$.

Here, d, p, q, d_{cp}, d_{cq}, F, and G are the client's secret information.

(2) The client sends plain messages M, D_s, and n to the server.

(3) The server selects one item, o_i, at random from term m, and applies the following illegality against term o_i:

$$o_i = -M^{d_i} \bmod n$$

Valid computations are applied to other terms o_j ($j \neq i$).

$$o_j = M^{d_j} \bmod n$$

(4) The server sends $O = [o_1, o_2, \cdots, o_m]$ to the client.

(5) The client calculates S_p and S_q with the following formulas:

$$S_p = M^{d_{cp}} \cdot \Pi_i o_i^{f_i} \bmod p$$

$$S_q = M^{d_{cq}} \cdot \Pi_i o_i^{g_i} \bmod q$$

Result S is obtained from S_p and S_q by means of the Chinese residue theorem (CRT). Namely, the following formula is calculated:

$$S = S_p \cdot W_p + S_q \cdot W_q \bmod n$$
where $W_p = q\ (q^{-1} \bmod p)$, $W_q = p\ (p^{-1} \bmod q)$.

The results obtained by the above are as follows:

$$S_p = (-1)^{f_i} \cdot M^d \bmod p = \pm M^d \bmod p$$

$$S_q = (-1)^{g_i} \cdot M^d \bmod q = \pm M^d \bmod q$$

Provided that F and G are selected at random, one of f_i and g_i becomes an odd number and the other becomes an even number, with a probability of 1/2. Under this condition, the server can obtain prime factors p and q of n by performing the operation in the next step, the description of which assumes that f_i is an even number and g_i an odd number.

(6) The server performs an exponentiation of S using public key e. Utilizing the fact that e is an odd number, the following formula can be obtained:

$$S^e = (W_p - W_q) \cdot M \bmod n$$

Next, $S^e + M \bmod n$ is calculated.

$$S^e + M = 2W_p\, M = 2M_q\, (q^{-1} \bmod p) \bmod n$$

If GCD (M, n) $\neq$ p, $2M\ (q^{-1} \bmod p)$ is not a multiple of p because $q^{-1} \bmod p < p$ and GCD (2, p) = 1. Therefore, GCD $(S^e + M, n) = 1$.

On the other hand, in case GCD(M, n) = p, prime factor p of n can be obtained by calculating GCD(M,n).

In case f_i is an odd number and g_i an even number, GCD $(S^e + M, n) = p$

3. Countermeasures

(1) Select proper acceleration protocol parameters

Select even numbers for all of the KS2 protocol parameters $f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_m$. This makes result S always valid whatever illegality the server performs on any term. With the S2 protocol, it is not possible to select even numbers for all of parameters $f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_m$. In this case, factorization attack can be prevented by aligning each f_i and g_i pair (i = 1, 2, $\cdots$, m) to produce an odd number or an even number.

(2) Select a proper checking method[3,4]

Perform checking by the direct checking method[3] and withhold any results that do not pass checking from external parties; this will make factorization possible.

4. Conclusion

The attack described in this paper consists of a factorization of public key n of the client, and is stronger than conventional attacks against RSA secret transformation acceleration operations. A valid countermeasure against such attacks is to set proper acceleration parameters. Knowing that there are also ways to attack accelerated computations that can cause factorization, it would appear to be necessary to introduce the concepts of zero-knowledge and nondiversion, which are attracting attention in relation to interactive demonstration-type protocols.

References

1. Matsumoto, T., Kato, K., and Imai, H., "Speeding Up Secret Computations With Insecure Auxiliary Devices," CRYPTO '88, Aug 88.

2. Kawamura and Shimbo, Fall 1980 IEICE National Convention, A-105, Sep 89.

3. Matsumoto and Imai, SHINGAKU GIHO ISEC89-4, May 89.

4. Shimbo and Kawamura, Ibid., ISEC89-5, May 89.

Development of Digital Signature With Error Position Detectability

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-288

[Article by Y. Fukuzawa, K. Takaragi, R. Sasaki, and T. Nakamura, Systems Development Laboratory, Hitachi, Ltd.; and H. Matsumoto, Hitachi Chubu Software, Ltd.]

[Text] **1. Introduction**

Digital signatures based on public-key cryptography[1] have the function of demonstrating the propriety of communication messages. In general, with a digital signature, hashed cryptography is performed to improve the signature efficiency of messages. The use of hashed cryptograms (hash total) can detect the presence of an alteration or error, but conventional methods have not been able to detect the position of the error.

This report describes a method for generating hashed cryptograms that makes it possible to detect the error position where the communication message has been altered, and assesses the effectiveness of this method.

2. Hashed Cryptogram Generation Method

The basic idea in generating hashed cryptograms with error position detectability is as shown in Figure 1.

(1) Communication message M is divided into S blocks M(i) ($1 \leq i \leq S$), and hashed cryptograms H(i) with a bit length of P are generated for each block divided.

(2) Hashed cryptograms H(i) are rearranged by changing their positions by m bits, and logical computation (XOR, for example) is performed to generate a hashed cryptogram DH with a bit length of W ($= P + m(S-1)$). In this operation, each of the hashed cryptograms obtained in step (1), H(i), is divided into HR(i) and HL(i). Should HL(i) and HR(j) exert influence on DH(k) ($1 \leq k \leq W$) which is any single bit of computation result DH, rearrangement is performed so that HR(i) and HL(j) do not exert an influence on any other bits DH(m) ($1 \leq m \leq W$, $K \neq m$).

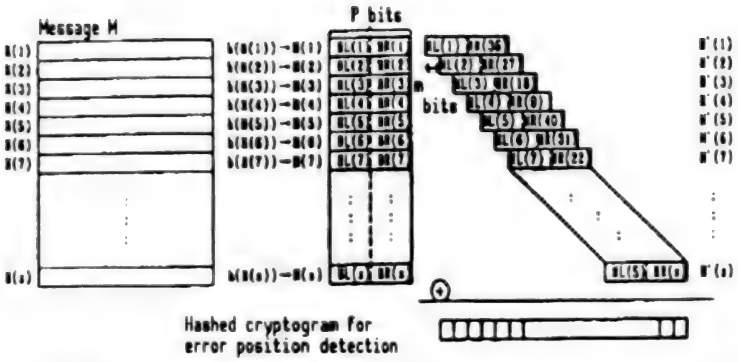


Figure 1. Generation Method of Hashed Cryptograms for Error Position Detection

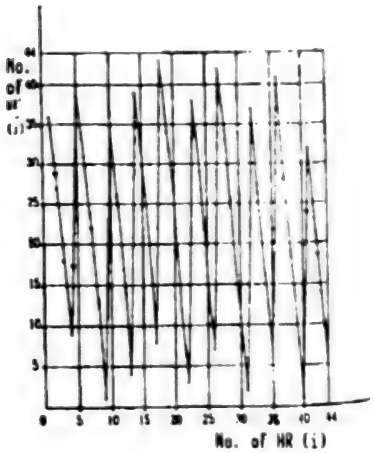


Figure 2. Example of Rearrangement

If an error occurs in the hashed cryptogram DH, the error position where the message is altered can be estimated by the following procedure:

Step 1: Blocks {M(i)} which could affect each DH(k) where error occurs are extracted, and the frequency that blocks M(i) appear in the bits of the extracted result is assumed to be N(i) ($0 \leq i \leq P$).

Step 2: When a communication message is altered, the probability that each of the corresponding bits DH(k) varies is in general one-half, and the statistics of the number of varied bits is in accordance with the binomial distribution B (P, one-half).

Therefore, N(i) is evaluated as the index of probability. As the value of N(i) increases, the probability that M(i) has been altered increases exponentially.

3. Concrete Example

An example of the rearrangement described above is shown below.

Assuming that: a) Left arrangement after rearrangement:

$$HL'(i) \leftarrow HL(i), \text{ and}$$

b) Right arrangement after rearrangement:

$$HR'(j) \leftarrow HR(i),$$

the rearrangement becomes as shown in Figure 2.

4. Evaluation

It is desirable that the length of hashed cryptograms created by a hash function be around 64 bits to ensure protection against round-robin search, and that the length of the digital signature obtained by means of public key cryptography be 512 bits or more to ensure protection against factorization and other attacks. Electronic identification technology "Hisecurity-V" proposes to use hashed cryptograms for communication messages, and to use other data, including date and time, as the original message for digital signature. Under this condition, it is possible to incorporate a hashed cryptogram of about 456 bits in an original message of 512 bits.

Based on the above, an evaluation was made using the following parameters: $s = 44$, $m = 8$, the partially hashed cryptograms were rearranged in a circle, and $W = 372$.

When the Davies-Price method[2] to which the common cryptosystem "Hisecurity-Multi"[3] is applied is used as the hash function, the generation of hashed cryptograms for error position detection took an additional post-processing time for rearrangement, etc., of 2.5 milliseconds in addition to the normal hashed cryptogram generation rate of 1.1 Mbps.

When 176-byte, fixed-format slip data were processed by this hashed cryptography technique under the conditions described above, the results showed that the data error position was detected as precisely as within 4 bytes if data were altered at only one position.

5. Conclusion

The authors believe that this method, which features error position detectability, is useful when several files are to be identified and transmitted together.

The next task is to evaluate the limit of the effectiveness in case errors are present in several blocks.

References

1. Ikeno and Koyama, "Modern Cryptography Theory," edited by IEICE, 1986.

2. Davies, D.W. and Price, W.L., "Digital Signature—An Update," 7th ICCC, 1984, pp 845-849.

3. Takaragi, et al., "Development of High-Speed Cryptography Algorithm Hisecurity-Multi 2 and Its Utilization," WCIS '89-D2.

4. Sasaki, et al., "Trend of Identification Technology in Trades Using Computer Network," JOURNAL OF IEICE, Vol 71 No 12, pp 1285-1287.

Constant-Envelope FFT Scrambler With Embedded Signal Power Information

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-290

[Article by T. Hasegawa, K. Komiyama, and Y. Hakura, Saitama University]

[Text] **1. Introduction**

The problem of information security has become more important than ever in the modern information society, FFT scramblingsl is an effective analog transmission privacy technique, but it still involves inherent weak points such as the fact that the accentuation of voice and information on syllables is maintained after scrambling because the envelope is maintained. Several measures have been taken to improve this point.[2,4]

The authors have previously proposed a method for providing a constant envelope by adding the voices of several people as simulated noise signals.[3] In this report, the authors propose and examine another constant envelope provision technique: an FFT scrambler with embedded signal power information. This technique provides a constant envelope by making the power of each transmitted privacy signal frame uniform, compressing the constant power information logarithmically, and embedding it in the spectrum section.

2. Proposal for FFT Scrambler With Embedded Signal Power Information

Figure 1 is a linear block diagram of the proposed method. The input voice is A/D converted, the RMS (root mean square) of each frame is calculated, and the signal power information is calculated so that the RMSs of the frames are constant. The information is then sent to the scrambler, at which time the audio signal is compounded so that the power is always constant. The signal is also fed to the FFT to be transformed into the frequency domain and, at the scrambler, its spectra are displaced to certain positions according to the scramble key. At this time, a predetermined spectrum is removed and logarithmically compressed power information is embedded in its place. The signal is then transformed back to the time domain by inverse FFT, and output as the transmitted privacy signal.

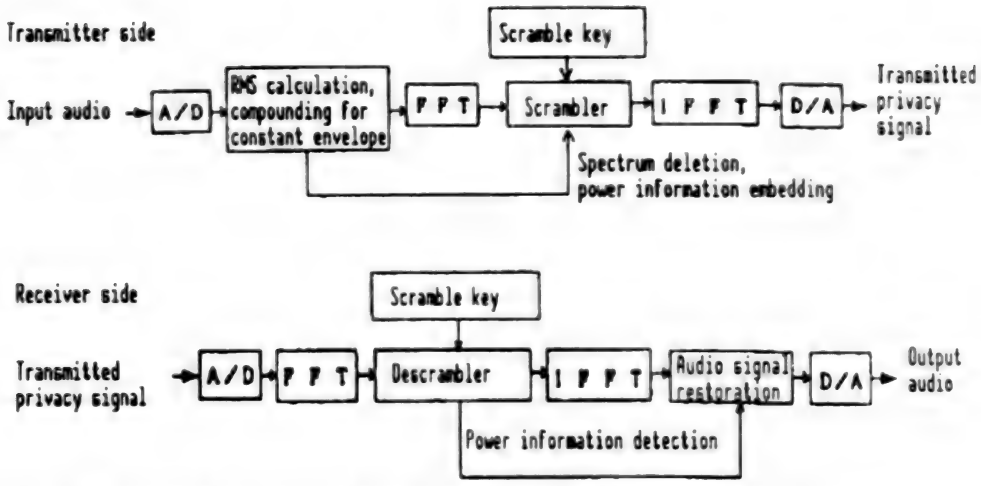


Figure 1. FFT Scrambler With Embedded Signal Power Information

At the receiver side, the embedded power information is extracted during the inverse displacement of the spectra. The missing spectrum is replaced with an average value derived from the adjacent spectra. After inverse FFT inverse compounding is performed based on the detected power information to restore the audio signal.

3. Computer Simulation

3.1 Experiment Specifications

The input audio is five seconds of a male voice. This signal is A/D converted with a sampling frequency of 10 kHz and 8-bit quantization, and simulation is performed at 1,024 samples per frame. The power information is embedded in place of the spectrum of the 2.0 kHz band, which is the band with the lowest voice energy.[4]

3.2 Results

The accentuation information of the transmitted privacy signal was undetectable, privacy was sufficient and the degradation of the reproduced voice was sufficiently low.

4. Conclusion

The authors propose an FFT scrambler with embedded signal power information, which provides a constant envelope by making the RMS value constant and which contains logarithmically compressed power information in the spectrum section. It has been demonstrated that this method provides a high degree of privacy with no accentuation information observed in the transmitted privacy signal.

Acknowledgements

The authors express their deep gratitude to Professor Misao Haishi of our university for his helpful advice.

References

1. Sakurai, Koga, and Muraya, "A Privacy Method," SHINGAKU GIHO, CS80-149, 1980, pp 1-6.

2. Tanaka, Shimizu, and Akiyama, "RINCOMPEX Scrambler," SHINGAKU RON, Vol J-70-B No 7, 1987, pp 894-896.

3. Hasegawa, Suzuki, and Hakura, "Analog Scrambler Improving Privacy by Means of Noise Signal Simulated From Voices," SHINGAKU GIHO, SSTAB 9-40, 1989, pp 33-37.

4. Torii, Higashi, and Matsuyama, "Trial Manufacturing of Prototype Constant-Envelope Spectrum Scrambler," SHINGAKU GIHO IN84-121, 1985, pp 31-36.

Pay Broadcasting Services Method Using Public Key Cryptosystem

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-291

[Article by Minoru Akiyama, Yoshiaki Tanaka, and Kenji Nishiyama, Faculty of Engineering, University of Tokyo]

[Text] **1. Introduction**

Following the diversification of broadcasting services in recent years, services available only to service subscribers who pay a charge (pay broadcast services) are being actively examined. However, if the key for restoring the image information is common to all subscribers, there is the possibility of illegal key distribution among the users. To prevent this, this paper proposes the use of a key not only for image restoration but also for the signature, using RSA cryptography.

2. Presupposition of the Proposed Method

To allow the use of a key in the signature, it is necessary to encrypt, using a different key for each subscriber, either whole or part of the image signal, the lack of which makes viewing impossible. This method presupposes the use of the latter (Figure 1).

However, the greater the number of subscribers, the greater the section designated #2* in Figure 1 should be. This problem can be solved by the method proposed in the next paragraph.

3. Proposed Method

Assuming that the number of signals in section #2 (signals whose minimum length is sufficient to make viewing impossible) to be encrypted is m and that the number of encryptions applied to each is n, the signal in which mn items of cryptograms are arranged is added to signal #1 and broadcast with it. To restore the original image, each subscriber's equipment performs n operations in which one of m signals encrypted with different keys is extracted and decrypted using the key he or she owns, and obtains m items for #2. To make this possible, m combinations of keys are supplied to each subscriber.

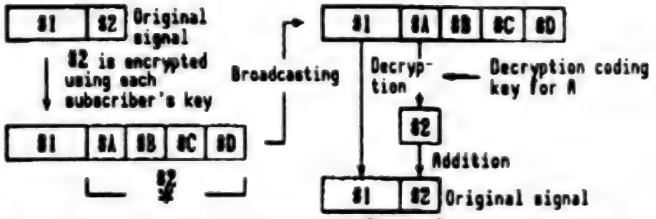


Figure 1. Scheme Presupposed for the Proposed Method

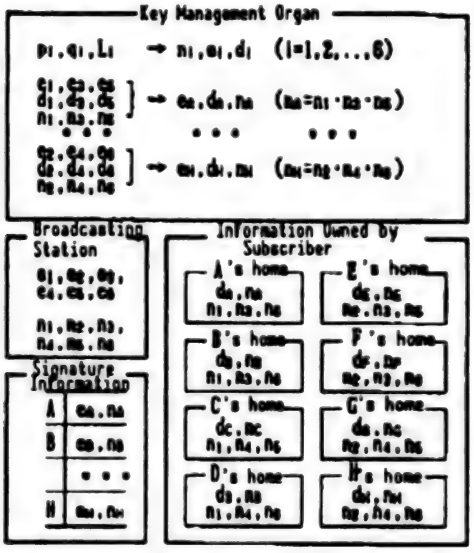


Figure 2. Information Owned by Key Management Organization, Broadcasting Station and Subscribers, and Information Required for Signature

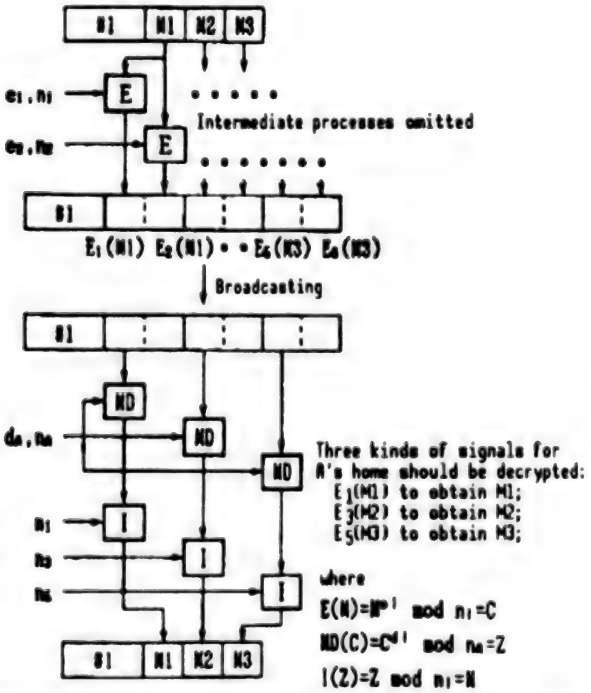


Figure 3. Outline of Operations of the Proposed Method (Example of A's home)

Figures 2 and 3 show an example when m = 3 and n = 2. In this example, the number of signals in section #2 which should be transmitted to the 8 (2^3) subscribers can be 6 (= 2 x 3) (it is conventionally 8). The following description is based on this example.

A reliable key management organization creates n_i, e_i, and d_i from six sets of large prime numbers (p_i, q_i), It selects three of these six keys as shown with the subscriber information in Figure 2, and combines them to generate the master key[1,2] (e_A, d_A, and n_A in case of subscriber A) of each subscriber (for use in place of an individual key). The reason why individual keys are not used is to prevent some subscribers from creating the key combination of another subscriber by offering a part of the key combination for each of them.

The keys are owned as shown in Figure 2. As the information for signature, a list of encryption master keys of each subscriber is made public.

Figure 3 shows the process of signal encryption and decryption. E stands for encryption, MD for decryption using the master key, and I for individualization.[2]

As the number of signals in #2 to be transmitted per number of subscribers N (= n^m) is mn, #2* in Figure 1 can be decreased by $e \cdot l_n N/N$ times.

4. Conclusion

For a pay broadcast service without illegal key distribution, the authors propose a method using public keys and master keys to replace individual keys.

References

1. Koyama, K., "Master Keys for RSA Public Key Cryptosystem," SHINGAKU RON (D), Vol J65-D No 2, Feb 82, pp 163-170.

2. Ibid., "Simultaneous/Distribution Cryptosystem Using Master Keys," Ibid., Vol J65-D No 9, Sep 82, pp 1151-1158.

Study of Security for Display TV by Time-Sharing Method

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-292

[Article by Shin Ohtake and Yoshinao Aoki, Faculty of Engineering, Hokkaido University]

[Text] **1. Introduction**

The authors propose a technique for CRT screen display that is legible only by the operator.[1] This paper describes the principle of this system, the results of an experiment using Japanese as the target font in addition to English, and the results of an experiment on the influence of the time-sharing method on legibility.

2. Principle of Security

Here, four text screen images are prepared. One of them contains the target text information, and the other three contain the masking information for obstructing the target. In this condition, the operation that opens the liquid-crystal shutter only for the period the target font is displayed and closes it when the mask fonts are displayed is performed in synchronization with the vertical sync signal (field divided, 60 Hz) (Figure 1).

Figure 1. View of Screen Display

This principle makes it possible to implement a CRT display image that is very difficult for third persons who do not have liquid crystal eyeglasses to read the target font on the CRT.

3. Experiments and Results

For this report, the following experiments were performed as supplements to our previous research:

1. Attesting effect on words composed only of Japanese Kanji characters compared to English words (uppercase).

2. "Flickering" due to opening and closing of liquid crystal shutter, and "illegibility" due to light dimming caused by time sharing.

In experiment 1, masked display images were shown to the subject, and the "reading-out period" was measured as the period from the moment a font is displayed until it was read.

In experiment 2, unmasked images were shown to the subject, and the reading-out periods were measured with and without the liquid crystal eyeglasses.

The following table shows these results:

Table 1. Legibility Rate and Influence of Time-Sharing Method on Reading-Out Period (The legibility rate refers to the percentage of subjects who succeeded in reading out.)

Experiment 1	English	Kanji word
Legibility rate (read words/total words)	1/100	8/100

Experiment 2	With glasses	Kanji
Average reading period (sec)	1.6	1.4

These results clarified the following points:

1. The effectiveness of this technique for ensuring the security of the displayed characters.
2. That Kanji characters are somewhat easier to read than English words.
3. Confirmation of the difficulty of reading the display image in the time-sharing method.

4. Conclusion

This report proposes a security technique for image displays and demonstrates its effectiveness with English words and Japanese characters. The authors are planning to study application technologies using this technique. Other themes for research include expanding the range of security from text images to graphic images, and, by advancing the concept of security by one more step, the time-shared use of large-screen and high-definition TV display images by several users.

References

1. Ohtake and Aoki, "Basic Experiments on Security of Display Characters Using Liquid-Crystal Shutter Eyeglasses," JOURNAL OF THE IEICE, to be included in CURRENT RESEARCH NEWS.

Proposal for Personal Identification System Based on Questions, Answers

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 1-293

[Article by Hiroyuki Hattori and Masao Mukaidono, School of Science and Technology, Meiji University]

[Text] In general, when a person uses a computer, the computer must be able to identify that person as one of the legal users. This used to be done mainly by using passwords. However, in case of computers used from remote locations, this method involves the danger of a disguised attack unless the communications path is secured.

This report proposes a new identification method based on fuzzy theory by making use of the difference of membership functions with respect to words.

1. Introduction

According to fuzzy theory, the concept of a word can be expressed with a membership function, and the membership functions can be simulated by a finite number of other membership functions.[1,2] Therefore, when simulating a required membership function using a finite number of membership functions for legal users who have been registered in the computer, it is only legal users or computers in which the membership functions of legal users have been registered that can obtain the simulated formulas. This system uses the membership functions of the legal users as secret keys to identify the legal users.

2. Identification Procedure

User identification is performed according to the following procedure.

<Procedure>

1) First, the user should register a finite number of symbols s1, s2, ..., sn and membership functions, $\mu s1$, $\mu s2$, ..., μsn, which correspond to the symbols in the computer. They should be stored so that they cannot be referenced by an external third party.

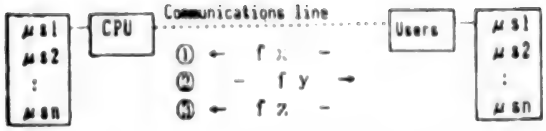


Figure 1. Outline of the Identification System

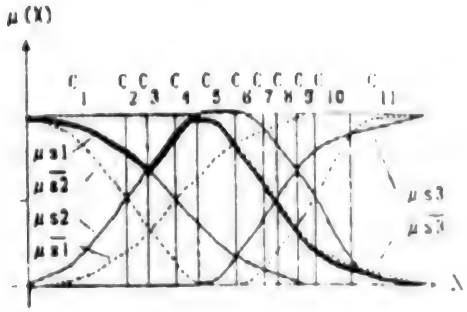


Figure 2.

2) A user utilizing the computer is identified as follows: When a user wants to utilize the computer, the user simulates a new membership function μx0, which has not been registered in the computer, using previously registered membership functions μs1 to μsn (the simulated membership function is assumed to be μxo'). The user then sends its simulated formula fx to the computer (Figure 1-(1)).

3) By substituting membership functions μs1, μs2, ..., μsn in fx sent from the user, the computer obtains the membership function originated by the user, μxo'.

4) The computer simulates an appropriate μyo, which meets condition (3) described later, using μs1, μs2, ..., μsn, and sends simulated formula fy to the user (Figure 1-(2)).

5) Upon receipt of fy, the user calculates formula fz, which represents μxo', using μyo.

6) The user obtains the simplest form of formula fz when the formula contains symbol yo of μyo.

7) The computer identifies the user as a legal user if formula fz sent from the user meets conditions (1) and (2) below.

Condition (1): When μyo and μs1, μs2, ..., μsn are substituted in fz, μxo' can be obtained.

Condition (2): fz shall be the simplest form when yo is used in the formula.

This system identifies users depending on whether formula fz containing yo is of the simplest form or not. This means that condition (3) below should be met when simulating μyo in step 4 of the procedure.

Condition (3): μxo and μyo shall match in one or more cell spaces.

3. Identification Example

Assume that membership functions $\mu s1$, $\mu s2$, and $\mu s3$ are determined for symbols s1, s2, and s3 as shown in Figure 2. When a user's concept is simulated by the membership functions represented by the thick curves in Figure 2, the simulated formula fx becomes as follows:

$$\mu xo' = \mu s1 \vee \mu s2 \cdot \mu\overline{s3}$$

$$fx \ : \ s1 \vee s2\cdot\overline{s3}$$

Next, the computer presents the user with the proper formulas, as shown below, which become tangential with $\mu xo'$ at C3 and C4 of Figure 2.

$$\mu yo = \mu s1\cdot\mu\overline{s2} \vee \mu s2 \vee \mu\overline{s1}$$

$$fy \ : \ s1\cdot\overline{s2} \vee s2 \vee \overline{s1}$$

Since the shapes of $\mu s1$, $\mu s2$, and $\mu s3$ are known, provided that the user is a legal user, $\mu xo'$ can be expressed by formula fz below using μyo.

$$fz \ : \ s1 \vee \overline{s3}\cdot yo$$

As this formula fz meets conditions (1) and (2), the user in question can be identified as a legal user.

4. Conclusion

This identification system exchanges information between users and the computer using symbols, while calculations by the users and within the computer are executed using membership functions. Thus, by substituting "words" for "symbols" and the "meanings of words" for "membership functions," if may be possible to identify users by conducting conversations using natural language between the computer and users.

References

1. Mukaidono and Takeda, "Simulated Expression of Fuzzy Information by Means of Fuzzy Logic Statements," Information Processing Society of Japan, "Knowledge and Artificial Intelligence," 41-5, 1985.

2. Mukaidono and Ohta, "Simulated Expression of Concepts Using Fuzzy Sets," 1988 National Convention of Japanese Electrotechnical Committee.

Feed Horn for C-Band VSAT Antenna

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-59

[Article by Kentaro Yamada and Matsuyoshi Iida, Microwave and Satellite Communications Division, NEC Corporation]

[Text] **1. Introduction**

The very small aperture terminal (VSAT) for the C band (4~6 GHz) has recently entered the stage of practical use. Compact antennas for use with VSAT must have small, lightweight feed horns. However, with the conventional low-order branching system in which the received signal is branched first, the receiving terminal should be projected orthogonally in the axial direction, and the size is restricted within an orthogonal cross section with the axis. In addition, it is necessary to incorporate a filter in the feed system in order to eliminate the impact on the LNA due to the transmitted signal, spurious signals, and thermal noise.

Therefore, by applying coaxial excitation and a ridge structure, the authors adopted a high-order branching system which branches the transmitted signal first. They also developed and implemented a compound feed horn incorporating filters in both of the terminals. This feed horn is the subject of this report.

2. Configuration and Functions

Figure 1 [not reproduced] shows an external view of the newly developed feed horn. As shown in Figure 2, it consists of: 1) a corrugated horn; 2) OMT; 3) HPF; and 4) TRF. It creates a TX/RX orthogonal linearly polarized wave. The transmitted signal is excited in the HPF by the coaxial probe, converted in the coaxial mode, excited in parallel with the ridge (in the direction of Ex) by the probe, and converted to the circular waveguide mode. The HPF consists of a cut-off filter with a cut-off frequency of 5 GHz. As shown in Figure 3, the received signal, whose main polarized wave is perpendicular to the ridge (in the direction of Ey) is led to the TRF with almost no effect from the ridge. The TRF is of the ridged, resonance post array type, which suppresses high-order mode excitation in the transmission band. For manufacturing, the

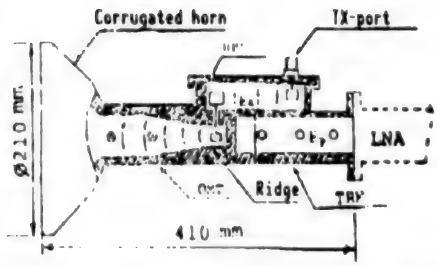


Figure 2. Horizontal Cross Section of Feed Horn

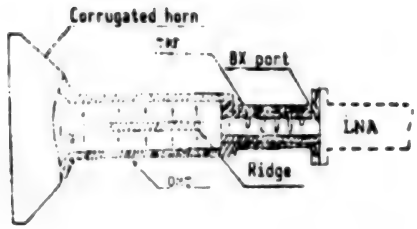


Figure 3. Vertical Cross Section of Feed Horn

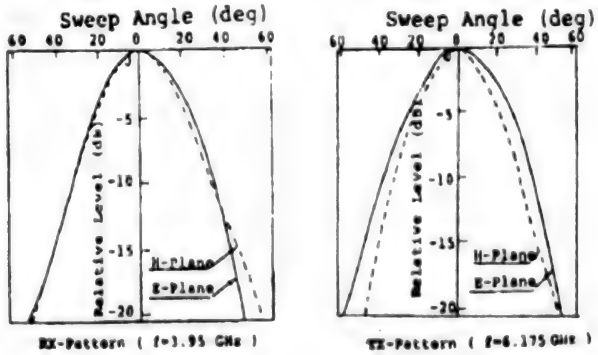


Figure 4. Radiation Patterns

lost wax process is used to cast the aluminum parts, so the weight is about 1.5 kg with the external specifications shown in Figure 2.

3. Characteristics

Table 1 shows the performance parameters of the feed horn. Figure 4 shows the radiation patterns of the transmit and receive bands of the feed horn.

Table 1. Electrical Performance Parameters

Frequency band	3.7~4.2 GHz	5.925~6.425 GHz
Polarized wave	Transmit/receive orthogonal linearly polarized waves	
VSWR	1.3	1.3
XPD	30 dB	30 dB
Loss	0.15 dB	0.35 dB

Port isolation	
3.7 ~4.2 GHz	85 dB
4.2 ~5.925 GHz	60 dB
5.925~6.425 GHz	80 dB

4. Conclusion

The authors have developed a feed horn based on the high-order branching system for use in a C-band VST antenna. The feed horn incorporates a TRF and HPF in addition to such basic components as the OMT and horn, thereby contributing to the simplification of the whole of the VSAT system. The feed horn is for use with 1.8 M to 2.4 M offset antennas.

S-Band Antenna for ERS-1

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-66

[Article by T. Ishida and N. Sugiura, National Space Development Agency; and H. Naka, S. Takayama, and Y. Yamasa, Toshiba Corporation]

[Text] **1. Introduction**

The authors have produced a prototype flight model (PFM) of the S-band antenna for telemetry command (TTC) to be mounted on the Japanese Earth Resources Satellite No. 1 (ERS-1), and have obtained satisfactory results from performance evaluation tests. The following is a report on this antenna.

2. Outline of Antenna

The ERS-1 is to be placed in a sun-synchronous, quasirecurrent orbit at an altitude of 570 km. The S-band antenna is to be mounted on the side of the satellite oriented toward the earth (+Yaw side). The S-band antenna is required to perform beam shaping in order to secure stable communication circuits within a field of ±66.7° of the +Yaw axis. As shown in Figure 1 [not reproduced] the shape is formed by a cross dipole and a circular reflector. Beam shaping is performed by adjusting the distance from the circular reflector to the cross dipole. Figure 2 is an installation of the S-band antenna mounted on the satellite.

3. Functions, Performance

The S-band antenna is used in the 2044.25 MHz band for transmission and the 2220.00 MHz band for reception, and both of the polarized waves are clockwise circularly polarized waves. Figures 3 and 4 show the gain patterns of the two frequencies. As shown in the figures, the patterns of both transmission and reception are very broad, covering wider fields than ±66.7° of the +Yaw axis. The size and shape are also determined by taking into consideration the structure when the antenna is mounted on the satellite and the need to prevent any influence from the payload equipment. An evaluation of the antenna patterns when the antenna is mounted on the satellite was performed using a one-fifth scale model.

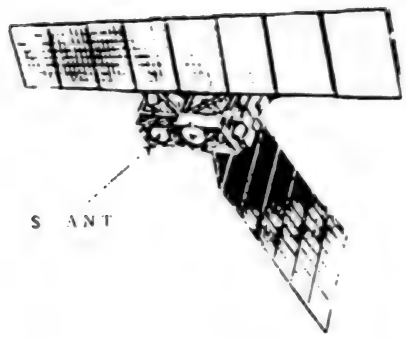


Figure 2. Mounting of S-Band Antenna on Satellite

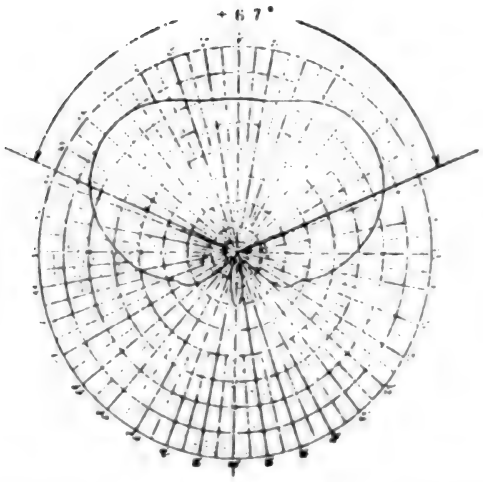


Figure 3. S-Band Antenna Radiation Pattern (2044.25 MHz)

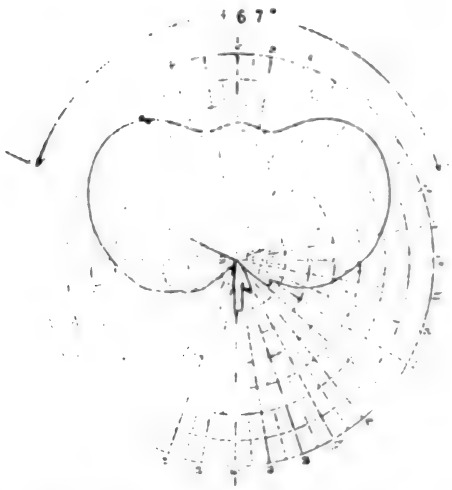


Figure 4. S-Band Antenna Radiation Pattern (2220.00 MHz)

Table 1. S-Band Antenna Performance Specifications

	2044.25 MHz band	2220.00 MHz band
Gain	-0.5 dBi or more within ±66.7° of +Yaw axis	-3.9 dBi or more on +Yaw axis 0.9 dBi or more within ±66.7° of +Yaw axis
VSWR	1.22 or less	1.19 or less
Polarized wave	Clockwise circularly polarized wave	Clockwise circularly polarized wave
Weight	805 grams	

This evaluation made it clear that the required patterns could be obtained even under influences of the satellite's structure, the solar battery paddle, the SAR antenna, etc. Environmental resistance evaluation tests of the antenna were also conducted in the launching and space environments, and favorable results were obtained. Table 1 shows the main performance specifications of the S-band antenna.

4. Conclusion

As stated above, it has been confirmed that this S-band antenna can meet the performance requirements for the ERS-1.

S-Band Intersatellite Communications Experiments Using ETS-VI

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-186

[Article by Shigeru Kimura, Yoshiaki Suzuki, and Masaharu Fujita, Communications Research Laboratory, Ministry of Posts and Telecommunications; and Masato Tanaka and Shigeo Yamada, National Space Development Agency]

[Text] **1. Introduction**

Japan's first intersatellite data relay experiments will use the S-band intersatellite communications (SIC) equipment mounted on the Engineering Test Satellite VI (ETS-VI), which is scheduled to be launched in 1993. The following is a summary of the experimental project.

2. Purpose of Experiments

The experimental project is aimed at acquiring the technologies necessary for the development of practical data relay satellites in the future through intersatellite data relay experiments between several satellites using the multibeam active phased-array antenna system developed as a payload for the ETS-VI.

3. Experimental System

Figure 1 shows the scheme of the S-band intersatellite communications experiments. The experimental system is composed of a manned spacecraft, such as a space base or JEM, user satellites (orbiter satellites at altitudes less than 1,000 km, such as a TDRSS user satellite), a feeder link station, and a simulated user station on the earth. Table 1 shows the main specifications of the system.

4. Experimental Project

The SIC system uses a phased-array system that uses two beams for reception and one beam for transmission. It accesses the user satellite by controlling the phase controller with the on-board microprocessor and scanning the beams electronically. In the return circuit (user satellite → relay satellite),

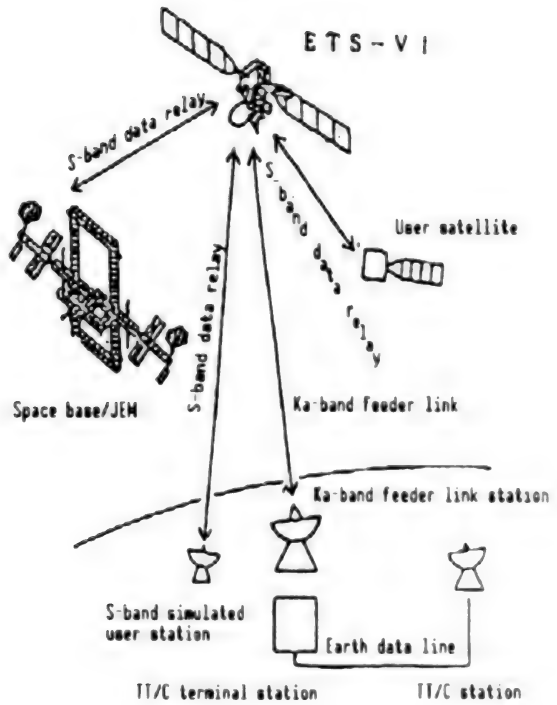


Figure 1. Outline of Communications Experiments Using ETS-VI

Table 1. SIC System Specifications

Frequency	Forward	2106.4 ± 3 MHz
	Return	2287.5 ±2.5 MHz
Data rate	~1.5 Mbps (TT/C, data, etc.)	
Modulation system	PN-PSK	
Bandwidth	6 MHz	
Field	20° (at an altitude less than 1,000 km from earth)	
Return circuit		
Antenna	19-element multibeam phased array	
Number of beams	2 (scanning beams)	
Gain	27.3 dB (minimum value within the field)	
Polarization	Counterclockwise circularly polarized wave	
Forward circuit		
Antenna	16-element multibeam phased array	
Number of beams	1 (scanning beam)	
Gain	26.2 dB (minimum value within the field)	
EIRP	34.1 dBW	
Polarization	Counterclockwise circularly polarized wave	

scanning is performed using two independent beams so multiple accesses from several user satellites are possible independently with a single channel. With the forward circuit (relay satellite → user satellite), scanning is performed using a single beam, which is used in a time-sharing manner with several satellites. The SIC system is designed to ensure compatibility with NASA's TDRSS system. The feeder link uses the 20~30 GHz band. The experiments can be divided into basic experiments and applied experiments. The basic experiments consist mainly of internal data relay experiments based on multiple access using user satellites, and the applied experiments include very-low-speed data transfer (a few bps or less). The actual experiments are listed in Table 2. Intersatellite data relay experiments are also planned using the Advanced Earth Observation Satellite (ADEOS) which will be launched in the future.

Table 2. Principal Experiments

Basic Experiments
(1) Intersatellite data relay experiments
(2) Intermembership function tracking and control experiments
(3) Phased-array antenna performance tests in space
(4) Communications with space base/JEM
Applied Experiments
(1) Very-low-speed data transfer experiments
(2) Space VLBI basic experiments
(3) Basic space surveillance experiments

5. Conclusion

The above is a summary of the S-band intersatellite communication experiments project using the ETS-VI, which is scheduled to be launched in FY 1993. These are the first intersatellite data relay experiments in Japan, and are attracting worldwide attention. At present, the payload as well as earth facilities for this project are being developed.

Acknowledgements

The authors express their deep gratitude to the organizations and firms concerned for their support and cooperation in the development of this project.

References

1. Ookubo, S., Itoh, T., Suzuki, Y., Tanaka, M., and Kitahara, H., "S-Band Intersatellite Communications Equipment System," KOKU UCHUGAKU, Vol 37 No 428

2. Suzuki, S., Yoshimura, K., Shiomi, T., Teyogi, T., Arimoto, Y., and Ariga, Ki, "Intersatellite Communications Experiment Project Using ETS-VI," 72nd CRL research announcement meeting, 1987.

3. Suzuki, Y., Yoshimura, K., Tanaka, M., Tanaka, R., and Kawanishi, T., "Intersatellite Communications Systems—Multibeam Communications and On-Board Signal Processing," Convention for the Federation of Electro-Information Association, 1989.

S-Band Intersatellite Communications Equipment for ETS-VI

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-187

[Article by Masato Tanaka and Yasushi Hatooka, National Space Development Agency; and Shigeru Kimura, Takeo Ito, and Masaharu Fujita, Communications Research Laboratory, Ministry of Posts and Telecommunications]

[Text] **1. Introduction**

S-band intersatellite communications (SIC) equipment is being developed for use in S-band multiple-access data relay systems. Such systems perform simultaneous data relay operations with several orbital satellites (user satellites) by handling low-speed and medium-speed data of a few kbps to 1 Mbps. The basic experiments are scheduled to be performed with the ETS-VI, which is scheduled to be launched in 1993. This report presents an outline of the SIC equipment.

2. Outline

The SIC equipment is intended for communications with user satellites at altitudes of less than 1,000 km above the earth. With antenna gain increased by using a spot beam to reduce the burden on the user satellite, it locates and tracks user satellites by electrical beam scanning using a phased-array design. The forward link (ETS-VI → user satellites) is used to relay commands. Since the amount of data carried by this link and its frequency of use are low, it uses a single beam that is time-shared by several user satellites, in a manner similar to NASA's TDRSS.[1] The return link (user satellites → ETS-VI) involves a larger amount of data, such as telemetry data and measuring data. As it is used more frequently, it uses two independent beams to access up to two user satellites. The performance of SIC equipment—such as the frequency, bandwidth, EIRP, and G/T—are made compatible with the S-band multiple-access (SMA) protocol of the TDRSS, thereby making it possible to perform mutual support experiments with the TDRSS. Table 1 shows the main specifications of the SIC equipment, and Figure 1 shows the configuration of the SIC equipment.

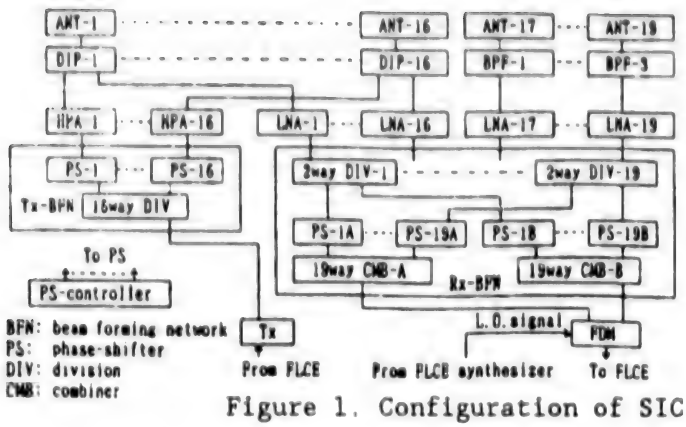


Figure 1. Configuration of SIC

Table 1. Main Specifications of SIC

Location and tracking performance	Tracking range	±10° (altitude of less than 1,000 km from the earth)	
	Antenna design	On-board beam forming, multibeam phased array	
	Number of beams	Forward link Return link	1 beam 2 beams
	Beam directivity error	Within ±0.6°	
	Tracking error	Within ±0.5°	
Communication performance	Frequencies	Forward link Return link	2.1064 GHz 2.2875 GHz
	Bandwidth	Forward link Return link	6 MHz 5 MHz
	EIRP	33.3 dBW	
	G/T	-4.4 dB/K	
	Polarization	Counterclockwise	

3. Features

(1) On-Board Beam Formation Method

The return antenna of the TDRS/SMA consists of a 30-element phased array. Regardless of the number of user satellites, it transmits the same number of received signals as there are receiving elements to the earth via individual feeder links, so the beam is formed on the earth. This method is suitable when there are several tens of object user satellites. It is superior in that it can reduce the burden on the relay satellite, because any complicated processing system can be located on the earth. However, with the SIC, as the number

of object satellites can be as small as a maximum of two, an on-board beam formation method[2] is used to form two independent beams by controlling two sets of phase shifter groups on the satellite. This allows the power needed by the feeder link to be reduced because the feeder link frequency band is only required to deal with the user satellites. This method also makes it possible to simplify the earth station. Problems presented by this method include the necessity to have the same number of phase shifters as (number of elements) x (number of beams), and consequently the phase shifter controller becomes more complex. However, attempts are being made to reduce their size and weight by implementing the phase shifter functions in microwave ICs (MICs) and the phase shifter controller function in an LSI.

(2) Active-Array Method

To improve reliability and reduce the size and power consumption of the power amplifiers and phase shifters, an active-array design is used in which a solid-state power amplifier (SSPA) and a low-noise amplifier (LNA) are connected to each antenna element. The increase of the number of SSPA and LNA devices accompanying this design is dealt with by reducing their weight by means of MIC implementation.

(3) On-Board Beam Directivity Control Method

Beam directivities are controlled by a microprocessor in the satellite. Control modes include a programmed tracking mode based on user satellite angle forecasts calculated on earth, and a mode with which the directivity is controlled based on simplified orbit calculations performed on the satellite for improved operational efficiency. There is also a beam directivity control mode in which the phase shifters are controlled directly by commands from the earth.

(6) Coherent Method

Although the SIC equipment and feeder link control equipment (FLCE) contain several frequency converters, the whole of the system, including the SIC equipment and FLCE, is configured coherently by utilizing the signals of the synthesizers inside the FLCE as the local oscillation sources for use in range rate measurement.

4. Conclusion

This article has described the functions and features of the S-band inter-satellite communications equipment to be mounted on the ETS-VI to make S-band multiple-access data relay possible. At present, the development model has been built, and it is being tested by incorporating it in an electrical model of the ETS-VI system.

References

1. Homes, W.H., Jr., AIAA78-554, 1978.

2. Chujo, et al., 31st Federation of Space Sciences, 1D/2.

Intelsat SSTDMA System Signal Processing Equipment

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-216

[Article by Yuuhei Ishi, Hidetoshi Hori, and Hiroshi Kimura, NEC Corporation; and Hideki Nakamura and Tatsuya Miwa, NEC Engineering, Ltd.]

[Text] **1. Introduction**

The authors have developed reference station equipment for the Intelsat SSTDMA satellite communications system and have succeeded in obtaining the required performance characteristics. The following is a report on this work.

2. Functions and Specifications

(1) TDMA transmission rate:	120.832 mbps
(2) TDMA and switch frame length:	2 ms
(3) Modulation/demodulation method:	4-phase absolute phase modulation/ coherent detection
(4) Network configuration:	2 reference stations, max. 54 slave stations
(5) Satellite timing synchronization:	
(5-1) Initial acquisition method:	Full-power acquisition by means of multiple-burst transmission
(5-2) Sync method:	Sent/received pattern comparison using metering bits
(5-3) Super-frame sync method:	Timing matching surveillance by UW modulation and switch state modulation

(6) Circuit surveillance and control functions:

(6-1) Circuit assignment change:	Simultaneous change within the network based on sync between reference station and satellite
(6-2) Reference station change:	Automatic activation according to network surveillance
(6-3) Slave station sync control:	Initial acquisition control and sync maintenance control by arranging sync bursts in sync control area

3. Configuration and Features

This equipment is used to deliver the reference burst to general stations, which form an SSTDMA network through the MSM (microwave switch matrix) mounted on the Intelsat VI satellite launched at the end of October 1989. The MSM timing sync function is incorporated in a unit called the ASU (acquisition and synchronization unit). At the same time as synchronizing the TDMA timing of the earth station with the switch frame timing of the satellite in the SSTDMA satellite communications system, this equipment also performs real-time monitoring and control of the stations participating in the TDMA. The equipment consists of a total of 13 racks: two SPE (signal processing equipment) racks; two ASU (acquisition and synchronization unit); one IF COMMON (IF signal common P equipment); five CADC (surveillance control equipment) racks; two ESC (prearrangement circuit control equipment); and one LTS (standard clock generator). In principle, the equipment operates with 1:1 redundancy. In case a fault occurs during normal operation, the active and standby systems are switched based on the self-diagnostics function or the control of the other reference station, thereby enhancing the reliability of the equipment.

The ASU rack incorporates a burst reception surveillance controller, which supervises the switching operations on the satellite. This improves the overall reliability of the network by supervising the receiving condition of all bursts received by a maximum of four down chains.

4. Conclusion

This equipment has already been tested using the satellite in its test orbit, and has been proved to have the required operational characteristics. The world's first commercial operations of Intelsat SSTDMA are scheduled in the Atlantic area before the end of 1990.

5. Acknowledgements

The authors express their deep gratitude to the persons concerned in the Intelsat SSTDMA project and KDD Meguro R&D Laboratories for their continuing guidance and cooperation in the development of the equipment.

Signaling Protocol Structure of Radio Link for Digital Mobile Communications Systems

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-342

[Article by Akira Kaiyama and Jun Tajima, Nippon Telegraph and Telephone Radio Communications System Laboratories; and Koji Yamamoto, Nippon Telegraph and Telephone Mobile Communications Division]

[Text] **1. Introduction**

The demand for mobile radio telephone services for portable or automobile use has increased rapidly in recent years, and it has become urgently necessary to increase the capacity and improve the economy of such mobile communications systems. Meanwhile, the diffusion of integrated services digital network [ISDN] services in fixed communications networks has also created a need for more diversified and more advanced services by mobile communications systems.

This report proposes a model signaling protocol structure of the radio link for digital mobile communications systems by applying the OSI reference model in the radio section (Um point) in order to provide additional functions as well as to meet the requirements described above.

2. Basic Policy in Proposing the Signal Protocol Structure

A model of the signaling protocol structure for the Um point in a digital mobile communications system is constructed according to the basic policy described below:

(1) Expandable signaling system, that can provide ISDN services as well as various mobile communications services.

(2) Signaling system with a reduced number of signals and shorter signal length for effective utilization of frequencies.

(3) Signaling system which assures the expandability of the system's functions by ensuring the separation of Layer 3 functional entities, that is, call control (CC), mobility management (MM), and radio frequency transmission management (RT), in compliance with CCITT and CCIR recommendations (Table 1).

(4) Signaling system which improves its flexibility as a protocol by ensuring the three-layer hierarchy of Layers 1, 2, and 3, according to the OSI reference model.

Table 1. Contents of Functional Entities

CC	MM	RT
• Bearer services • Teleservices • Additional services, etc.	• Position registration • User identification, etc.	• Radio circuit control (assignment release), etc.

3. CC/MM/RT Separation and Multiplexing Method

The Layer 3 functional entities, which are independent with respect to others, may be multiplexed by one of three methods: Layer 1 multiplexing, Layer 2 multiplexing, or Layer 3 multiplexing. Of these, the Layer 1 multiplexing and Layer 2 multiplexing are advantageous in terms of achieving good CC separation thanks to the mobile equipment configuration method, the absence of influence of CC changes on the mobile equipment, and the possibility of implementing mobile equipment functions in a small unit. But their large signal lengths are disadvantageous when considering the transmission of I interface signals. In contrast, the Layer 3 multiplexing method is disadvantageous because of the heavy burden placed on the mobile equipment because the CC Layer 3 should be terminated in the mobile equipment. However, considering the fact that the transfer capacity of the ACCH (auxiliary control channel) of digital mobile communications systems is around some hundreds of bits per second, this method is desirable because it can compress the CC signal.

4. Signal Structure

The signal structure complies with the OSI reference model. It consists of a three-layer hierarchy with Layers 1, 2, and 3. From the viewpoint of effective frequency utilization—particularly in the CCCH (common control channel)—a sharing mechanism is required in Layer 3 to make it possible to reduce the number of signals (Figure 1).

5. CC Signal Sequence

For the basic connection, the I sequence is applied for connections with I terminals. For additional services, it is not realistic to support only the I sequence in the digital mobile communications system when the delay time is considered based on the transfer capacity of the ACCH. Therefore, they are divided into a part for mobile use, which supports a sequence with a reduced number of signals, and a part supporting the I sequence in consideration of the connection of I terminals.

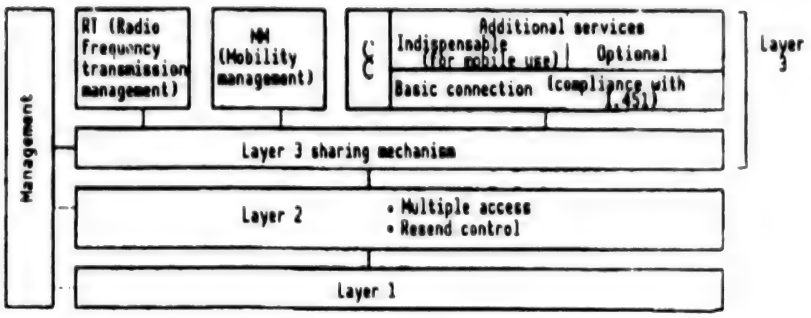


Figure 1. Outline of Signal Structure

6. Conclusion

In the above, the authors have proposed a signaling protocol structure for radio links in digital mobile communications systems.

References

1. Nakamura, et al., "Call Control Signaling Protocol Structure on Radio Link for Digital Mobile Communications Systems," 1990 IEICE National Convention.

2. CCITT Recommendations Q.1061, Q.1063.

3. TCC, TCC Standard "User-Network Interface," Vol II, Part 1.

Transmission Properties of G4 Facsimile on Mobile Satellite Communications Channel

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 2-252

[Article by Haruo Kondo, Hiroyuki Wajima, Hitoshi Komagata, and Takeio Atugi, Nippon Telegraph and Telephone Radio Communications System Laboratories]

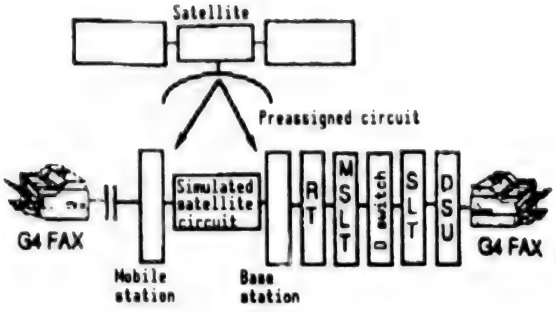
[Text] **1. Introduction**

To ascertain if it is possible to create integrated services digital network (ISDN) services using digital mobile communications systems in the future, the authors carried out a series of experiments to check the I terminal connection operations[1] as a part of the EMSS experiments. This paper reports on the transmission properties of G4 facsimile terminals identified in the indoor and marine experiments.

2. Experimental System Configuration and Transmission Sequence

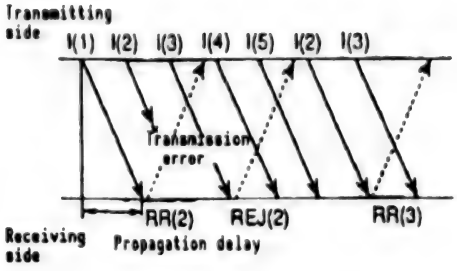
Figure 1 shows the configuration of the experimental system, and Table 1 lists its specifications. The indoor experiments involved inserting a delay in the radio circuit and the absence of fading (see below). The marine experiment involved mounting a 3 x 3-element microstrip antenna on Nippon Telegraph and Telephone's (NTT's) submarine cable laying vessel, the "Kuroshio Maru" (3,600 tons), in the route between Yokohama and Hawaii.

Figure 2 shows the G4 facsimile transmission protocol (which performs resend by returning to the frame where the error occurred). In these experiments, a transparent circuit was established between the mobile station and the base station, and the information packet length, period required for the transmission of an A4 sheet and the transmission completion percentage were measured.



RT: remote multiplexing terminal
SLTE: subscriber line terminal equipment
⊣ ⊢ : Basic interface
MSLT: multiplexed subscriber line terminal
DSU: digital subscriber line terminal unit

Figure 1. Configuration of Experimental System



_____ I(m): Information command frame (m; send sequence No.)
- - - RR(n): Receive-enabled response frame (n; receive sequence No.)
Number of outstanding frames = 7
(Frames which can be transferred without confirming the response signal)

Figure 2. G4 Facsimile Transmission Sequence

Table 1. Specifications for Experimental System

Radio circuit signal rate	330 kbps
Modulation/demodulation	OQPSK, absolute sync detection
Error correction	Rate 1/2, constant length 4, convolutional encoding/Viterbi decoding
Interface between mobile station and F4 facsimile	2B+D basic interface

3. Experimental Results

Figure 3 shows an example of the average transmission time. The number of initially sent packets per A4 sheet is about 280 with a packet length of 128 bytes, about 130 with 256 bytes, and about 75 with 512 bytes.

(Indoor experiments)

Figure 2 shows that the transmission time becomes shorter as the packet length becomes longer. This is because, if the information packet length is short, the transmitter side cannot send more information frames than the number of outstanding frames within the two-way propagation delay period and there will

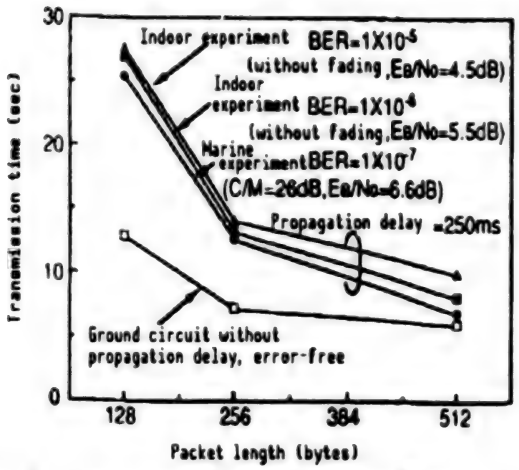


Figure 3. Average Transmission Time

be a waiting period until the answer signal reaches the transmitter side. The transmission completion rate was 100 percent with a bit error rate (BER) of less than 10^{-5}.

(Marine experiment)

Because a tracking-type directivity antenna was used as the mobile station antenna, the influence of fading due to vessel vibration was small and the C/M (power ratio between the direct wave and the reflected wave) during the experiment was about 26 dB. The transmission time was equivalent to that of ground circuits when the packet length was 512 bytes.

4. Conclusion

Our experiments confirmed that the image transmission properties of a G4 facsimile using a satellite circuit can be almost equivalent to ground circuits provided that the BER of the transmission channel is about 10^{-6}.

In closing, the authors would like to express their thanks to the director of the Communications Satellite Technology Research Department of the Radio Communication Systems Laboratories and the persons concerned for their daily guidance in our research.

References

1. Miyajima, et al., Report in 1989 IEICE National Convention.

2. CS Experiments General Report, May 83, pp 163-168.

Study on Broadcasting Satellite Service in 22 GHz Band

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p p-590

[Article by Kouzou Kameda and Tetsuo Yamamoto, NHK Science and Technical Research Laboratories]

[Text] **1. Introduction**

Satellite broadcasts currently use the 12 GHz band, and the 22 GHz band is regarded as the next frequency band that will be used for satellite broadcasting. However, only limited research has been done on this frequency band,[1,2,3] and many subjects, including frequency allocation, have not been studied. This paper reports the results of a study made by the authors on frequency allocation for 22 GHz band satellite broadcasts, also taking future broadcast services and high-reliability digital transmission systems into consideration.

2. Broadcasting Services

It is desirable that the services in the 22 GHz band not be simply additional channels to the 12 GHz band, but that they offer new types of broadcasting services for the future by providing a broader band based on an understanding of the properties of the medium. However, in considering the contents and transmission schemes of the services, it should be noted that attenuation caused by rain is high in the 22 GHz band. The services transmitted may include the following: 1) enhanced definition television (EDTV) digital transmission; 2) high-definition television (HDTV) analog transmission; 3) broadband integrated services digital network (ISDN); and 4) small-capacity digital transmission (VSAT).

3. Transmission Scheme

The EIRP control technique is considered to be a countermeasure against large rainfall attenuation, but a high-reliability modulation/demodulation system is effective as well. An example of such a system is a system that uses Viterbi decoding with convolutional codes. With services 1) and 3) above, for example, the information capacity is 130-150 Mbps and the transmission capacity is 150-300 Mbps, assuming that the encoding rate, r, is between 1/2 and 7/8.

4. Channel Arrangement Plan

Assuming the use of an effective frequency utilization scheme similar to existing systems based on polarized wave identification, when the width of 500 MHz (22.5-23 GHz) is divided into eight channels, the bandwidth of each channel is about 100 MHz. Therefore, the lowest value of the transmission capacity (about 150 Mbps) can be achieved by 4-phase PSK.

5. Circuit Design

Table 1 shows examples of a 150 Mbps, 4-phase PSK circuit design with six 90 W beams (satellite output 540 W) or one 400 W beam. The rainfall attenuation is estimated to be 9 dB (time rate 99 percent in the worst month) or 5 dB (time rate 95 percent in the worst month). The required C/N is 12.3 dB, and valid circuits re obtained from both designs.

Table 1. Examples of Circuit Design

(a) 90 W, 6-beam DOWN LINK		Time rate 99%
Frequency	(GHz)	22.75
Satellite transmission power	(W)	90.00
Transmitting antenna diameter	(cm)	260.00
Beamwidth	(deg)	0.35
Feeder loss	(dB)	2.30
Transmitting antenna gain -3 dB	(dBi)	50.62
Pointing loss	(dB)	0.40
Effective radiated power	(dBW)	67.46
Free space loss	(dB)	211.16
Rainfall attenuation	(dB)	9.00
Receiving antenna diameter	(cm)	60.00
Antenna efficiency	(%)	70.00
Receiving antenna gain	(dBi)	41.55
Receiver input C	(dBW)	-111.14
Boltzmann constant		-228.60
Antenna noise temperature	(K)	260.00
Receiver NF	(dB)	2.00
Receiver noise temperature	(K)	169.62
Receiving system noise temperature	(dBK)	26.33
Nyquist receiving bandwidth	(MHz)	75.00
Noise power N	(dBW)	-123.52
C/N Nyquist	(dB)	12.38
Required C/N Nyquist*	(dB)	12.30
Margin	(dB)	0.08

*1 x 10^{-6} after error correction
Including fixed degradation of 3 dB

[Table 1 continued]

[Continuation of Table 1]

(a) 400 W, 1-beam DOWN LINK		Time rate 95%
Frequency	(GHz)	22.75
Satellite transmission power	(W)	400.00
Transmitting antenna diameter	(cm)	60.00
Beamwidth	(deg)	1.80
Feeder loss	(dB)	2.30
Transmitting antenna gain -3 dB	(dBi)	40.88
Pointing loss	(dB)	0.00
Effective radiated power	(dBW)	64.61
Free space loss	(dB)	211.16
Rainfall attenuation	(dB)	5.00
Receiving antenna diameter	(cm)	60.00
Antenna efficiency	(%)	70.00
Receiving antenna gain	(dBi)	41.55
Receiver input C	(dBW)	-110.00
Boltzmann constant		-228.60
Antenna noise temperature	(K)	260.00
Receiver NF	(dB)	2.00
Receiver noise temperature	(K)	169.62
Receiving system noise temperature	(dBK)	26.33
Nyquist receiving bandwidth	(MHz)	75.00
Noise power N	(dBW)	-123.52
C/N Nyquist	(dB)	13.52
Required C/N Nyquist*	(dB)	12.30
Margin	(dB)	1.22

*1 x 10^{-6} after error correction
Including fixed degradation of 3 dB

6. Conclusion

The authors studied the services, transmission scheme and channel arrangement for 22 GHz band satellite broadcasting, and designed appropriate circuits. Their next task is to study the frequency allocation based on their interference calculations.

References

1. Kato, et al., "Study of 22 GHz Band Satellite Broadcasting Systems," IEICE NEWS, SANE89-2, Jun 88, 97-12.

2. Miyasaka, et al., "A Consideration of 22 GHz Band Satellite Broadcasting," IEICE NEWS, SANE89-35, 1989.

3. Yoshimoto, et al., "A Study of 22 GHz Band Regional Satellite Broadcasting Systems," JOURNAL OF IEICE, Vol j69-B.

Encrypted Transmission Scheme for Signals Generated Using Variable-Length Encoding

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-253

[Article by Hideki Tsubakiyama and Hideo Okinaka, KDD Meguro R&D Laboratories]

[Text] **1. Introduction**

The bandwidth used for the digital transmission of an image signal, etc., is often compressed by means of variable-length encoding. This report proposes an encrypted transmission scheme for signals generated by variable-length encoding, with which fast resynchronization is possible after clock loss or clock slip during transmission.

2. Proposed Transmission Scheme

In the proposed scheme, signal sequences generated by variable-length encoding are encrypted and transmitted using the procedure shown in Figure 1. The sync pattern in the original signal is replaced by the sync signal for transmission, SYN(n) = A(n-1)+a (Step 1). Signal sequences other than the sync signal are then encrypted using a desired cryptosystem (Step 2), and one bit from b is inserted after every signal sequence A(n-1) appearing in the encrypted part of the information to prevent the generation of false SYN(n) (Step 3). Here, SYN(n) is a fixed pattern with n bits, A(N-1) is a fixed pattern with (n-1) bits, a is one bit (either "1" or "0"), and b is XOR of a and "1." The encryption in (Step 2) uses a system in which initialization is performed for every sync signal.

In the proposed scheme, synchronization between encryption and encoding is established by the sync signal for transmission. Thus, fast resynchronization is possible even when a clock slip or clock loss occurs due to noise or momentary power failure.

If the length of the sync signal for transmission obtained by the operation in (Step 3) is equal to the length of the sync signal in the original signal, the amount of data after encryption becomes larger than the original amount of data. However, the problem of increased data can be avoided by setting the

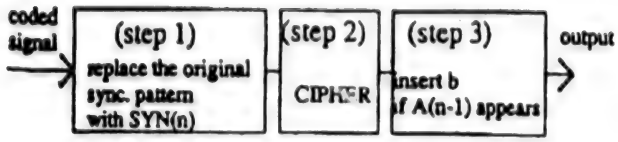


Figure 1. Proposed Scheme

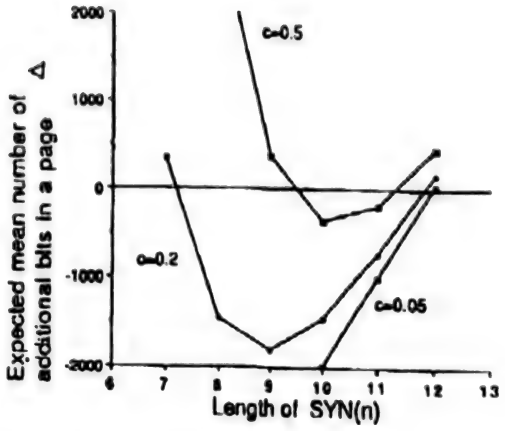


Figure 2. Amount of Transmitted Data Increase

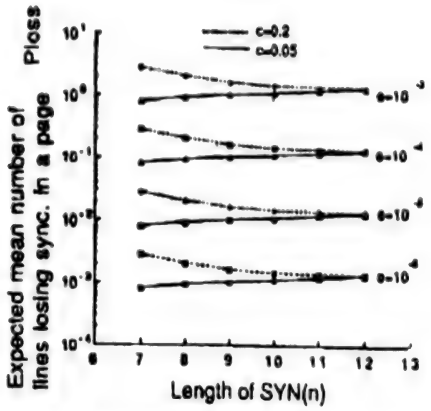


Figure 3. Number of Lines Losing Sync

length of the sync signal for transmission so that it is shorter than the length of the sync signal in the original signal, assuming the sync characteristics permits this.

3. Application of G3 Facsimile

A G3 facsimile signal is composed of a control signal, which determines the transmission procedure, and an image signal, which is encoded. This encoded image signal is in turn composed of image data generated by variable-length encoding of the EOL and MH codes in a synchronized fixed sequence. This is done so that the proposed encrypted transmission scheme can be applied.

Figures 2 and 3 show the increase in the amount of transmitted data and the sync error rate with respect to the length of SYN(n) when the proposed scheme is applied. By setting the length of the sync signal for transmission to 11 bits, for example, the amount by which the transmitted data increases is negative (the compression rate, c, for G3 facsimile encoding is reported to be between 0.05 and 0.2[1]) so statistically there is no degradation of transmission efficiency due to encoding.

4. Conclusion

The proposed encrypted transmission scheme for signals generated by variable-length encoding features fast resynchronization after the occurrence of clock slip or clock loss. It can be designed to statistically suppress the

degradation of transmission efficiency due to encryption, and can select any encryption algorithm desired.

Acknowledgements

The authors express their gratitude to Director Koga of the Transmission Signal Processing Laboratory of the Meguro R&D Laboratories.

References

1. "Image Communication Technology," KEC, 1982, compiled by Nakagome, p 96.

Method for Spread-Spectrum Multiplex Communications Using Synchronizing Signal of Power Line Frequency

916C3801 Tokyo DENSHI JOHO TSUSHIN GAKKAI SHUNKI ZENKOKU TAIKAI in Japanese Mar 90 p 3-271

[Article by S. Kiba, T. Takezawa, Y. Taniwaki, T. Kurosawa, and H. Hirose, Nippon Institute of Technology]

[Text] **1. Introduction**

The authors have studied a method for simplifying the spread-spectrum (SS) multiplex communications system by utilizing the power line frequency as the sync signal of the SS communications system. This system uses the CDMA scheme, but the codes assigned to each channel are shifted by one chip or more with respect to the same code source. This makes it possible to produce smaller spread code generation, and synchronization equipment, and to reduce inter-channel interference thanks to a lower cross-correlation between spread codes. This report deals with SSMA equipment that makes use of this system.

2. Principle

It is well known that, assuming that a serial code with a code length of m is defined as

$$(a_i) = (a_0, a_1, \cdots a_{n-2}, a_{n-1}),$$

its self-correlation function is 1/n, except when the codes are within ±1 bit, and that it has a triangular shape centered around the 0 bit. In general, synchronization is assured by utilizing this property. For the system where synchronization is assured with respect to the power line frequency, the cross-correlation of codes shifted by one chip or more is 1/n. Therefore, as the interchannel interference of codes assigned to different channels is low, the number of assigned channels is equal to the code length n, taking only the correlation value into consideration. However, it is actually smaller than n because of the cycle-and-add property of the m serial codes.

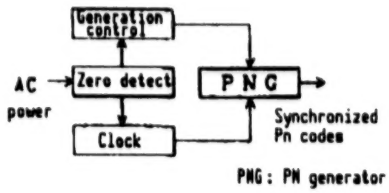


Figure 1. Power-Synchronized PN Code Generator

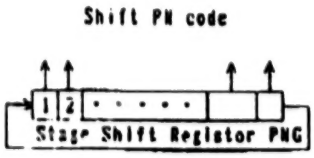


Figure 2. Shifted PN Code Generator

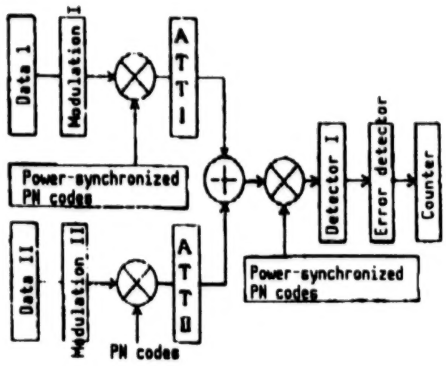


Figure 3. Measuring System

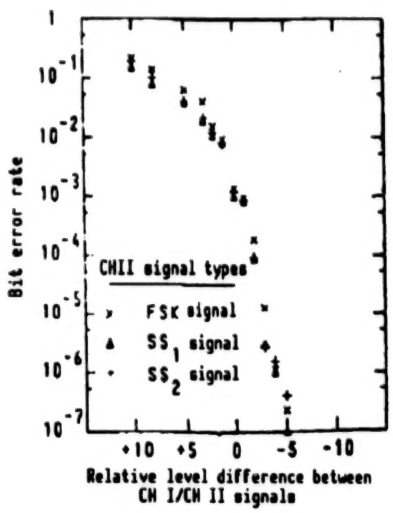


Figure 4. Relative Level Difference Between CH I/CH II Signals Versus CH I Bit Error Rate

3. Transmitter/Receiver Configuration

The SS multiplex communication equipment synchronized with the power line frequency that we developed has two channels. The 10.7 MHz carrier is modulated by FSK by the NRX signal with a transmission data rate of 2,400 bps, then spread by 255-bit m serial codes with a chip rate of 2 MHz.

4. Measuring System

Test data is applied to CH I, and the signal of the other channel, CH II, is mixed in its transmission path. This signal consists of the SS_1 signal using codes shifted by one bit or more; the FSK signal, which is not spread; and the SS_2 signal, which uses m serial codes that are different from CH I. Then, for each of these signals, the relative difference of CH II with respect to the reference CH I and the bit error rate in CH I are measured, and their relationship is evaluated.

5. Experimental Results

Figure 4 shows the results of the measurements of the relative level difference measurement and CH I bit error rate of each type of CH II signal.

6. Conclusion

The experiment clarified the properties of SS multiplex communication equipments synchronized with the power line frequency using spread codes shifted by one bit or more. The next step will be to measure the properties when the number of channels is larger.

References

1. Kurosawa, Hirose, and Furuhashi, Report in 1989 IEICE National Convention, SP-8-10.

- END -

END OF FICHE DATE FILMED

15 April 1991